

UNIVERSITÉ PARIS I PANTHÉON SORBONNE
ED de droit comparé

Laboratoire de rattachement : Institut de recherche juridique de la Sorbonne
(IRJS)

THÈSE

Pour l'obtention du titre de Docteur en droit comparé

Présentée et soutenue publiquement

le 17 décembre 2024 par

Shathil NAWAF SHATHIL

**LA PROTECTION JURIDIQUE
DES DOSSIERS PASSAGERS**

Sous la direction de M. William GILLES

Maître de conférence HDR à l'Université Paris 1 Panthéon-Sorbonne

Membres du jury :

Antoine Delblond, Professeur de droit public à l'Université de Nantes (rapporteur)

María Belén Andreu Martínez, Professeur titulaire de droit à l'Université de Murcie
(rapporteur)

William Gilles, Maître de conférences HDR en droit public à l'Université Paris 1 Panthéon-Sorbonne, Directeur de recherche

Jacqueline Morand-Deville, Professeur émérite de droit public à l'Université Paris 1 Panthéon-Sorbonne

Jean-Claude Beaujour, Docteur en droit, Avocat, Président de la Commission aviation de l'Inter Pacific Bar Association (IPBA) et Secrétaire général de l'Institut français des experts juridiques internationaux (IFEJI)

Avertissement

L'Université Paris 1 Panthéon-Sorbonne n'entend donner aucune approbation, ni improbation aux opinions émises dans les thèses ; ces opinions doivent être considérées comme propres à l'auteur.

À ceux qui ont sacrifié leur vie pour moi, mes parents

Remerciements

Au terme de ces six années de recherche, je tiens à exprimer ma profonde reconnaissance à M. William Gilles, mon directeur de recherche, pour son soutien bienveillant, sa disponibilité et ses précieux conseils, ainsi que pour la confiance qu'il m'a accordée. Aux côtés de Mme Irène Bouhadana, ils m'ont offert l'opportunité de participer à des séminaires et colloques internationaux, favorisant des échanges enrichissants avec des chercheurs du monde entier.

Mes remerciements les plus chaleureux vont également à Mohamed Sadek pour son soutien infaillible en tant qu'ami et collègue doctorant, ainsi qu'à Julie Boisard-Pétrissans pour ses précieux conseils. Je tiens également à exprimer ma gratitude à Dr. Ibrahim Al Aqidi, Alia Mamdouh, Gen. Abdulaziz Al Ansari et Dr. Nasser Hinzab pour leurs encouragements constants.

Je dédie cette thèse à la mémoire de Dr. Nabil Al Azzawi, Dr. Riyadh Al Wayes et Dr. Riyadh Al Qaisi, dont l'inspiration a marqué mon parcours.

Enfin, je remercie ma famille, dispersée à travers le monde, pour son soutien malgré la guerre et la distance.

Résumé

Les attentats du 11 septembre 2001 ont profondément bouleversé les sociétés occidentales. Le transport aérien international mais également plusieurs branches du droit, dont le droit pénal et le droit des libertés publiques, ont été affectés. Le droit américain a imposé aux compagnies aériennes la transmission des données personnelles des passagers aériens, appelées Passenger Name Record (PNR). Alors que les États-Unis exigent cette transmission pour des raisons de sécurité nationale, le droit européen privilégie la protection de la vie privée et des données personnelles. Bien que l'accord euro-américain et d'autres accords similaires, ainsi que la directive européenne sur les PNR, visent à encadrer les échanges de données, ils sont susceptibles de porter atteinte aux droits fondamentaux des passagers. Cet équilibre entre sécurité et droits individuels se heurte à une réalité juridique : une limitation des libertés au nom de la sécurité collective. Tandis que le Conseil et la Commission européenne prônent des mesures sécuritaires, le Parlement européen et la Cour de justice de l'Union européenne cherchent à préserver les libertés individuelles. De nouvelles menaces pèsent sur la protection juridique des dossiers passagers telles que la collecte massive de données et le profilage aux frontières. L'intervention croissante des acteurs privés, notamment dans les aéroports, affaiblit cette protection et la déterritorialisation des données accentue cette vulnérabilité. Les crises internationales, comme la pandémie du coronavirus, ont encore renforcé l'usage de ces données, compliquant leur encadrement juridique.

Mots-clés

aéroport - données des dossiers passagers - données personnelles - droits fondamentaux - États-Unis - passagers - PNR - protection - sécurité collective - terrorisme - transport - Union européenne - aérien

Summary

The terrorist attacks of September 11, 2001, significantly disrupted Western societies. International transport law, along with areas of law such as criminal law and public freedoms, were profoundly affected. U.S. legislation imposed an obligation on airlines to transmit the personal data of air passengers, referred to as Passenger Name Record (PNR). While the U.S. requires this transmission for purposes of national security, European law prioritizes data protection. Despite the aim of the Euro-American agreement, other bilateral accords, and the European PNR Directive to regulate data exchanges, they pose a risk of infringing upon passengers' fundamental rights. This legal balance between security and individual rights reveals a tension: the restriction of civil liberties in the name of collective security. While the European Council and Commission endorse security-focused measures, the European Parliament and the Court of Justice of the European Union (CJEU) seek to uphold individual liberties. Emerging threats to the legal protection of passenger data include mass data collection and profiling at borders, which are at odds with privacy rights. The growing involvement of private actors, particularly in airports, further undermines this protection, while the de-territorialization of data exacerbates its vulnerability. Additionally, international crises such as the COVID-19 pandemic have led to an expanded use of passenger data, complicating its legal regulation and oversight.

Keywords

airport - data protection - European Union - individual rights - passengers - personal data - PNR - protection - security - terrorism - transport - United States

Sommaire

Partie I – Les limites traditionnelles à la protection juridique des dossiers passagers

Titre 1 – La prééminence des législations répressives en matière de dossiers passagers

Chapitre 1 – L’antagonisme entre les législations répressives relatives à la transmission des dossiers passagers

Section 1 – L’obligation de transmission imposée par le droit américain

Section 2 – La contestation opposée par le droit européen

Chapitre 2 – Le consensus des législations répressives sur la finalité sécuritaire des dossiers passagers

Section 1 – Un consensus illustré par l’existence d’un accord euro-américain sur le transfert des dossiers passagers

Section 2 – La présence de la logique répressive américaine dans la directive européenne sur les dossiers passagers

Titre 2 – L’empiètement des législations répressives sur les droits fondamentaux des passagers aériens

Chapitre 1 – Les accords PNR, un échange des dossiers passagers sans protection juridique effective

Section 1 – L’empiètement reconnu sur le droit au respect à la vie privée et sur le droit à la protection des données personnelles

Section 2 – La limitation des droits fondamentaux au nom de la sécurité publique

Chapitre 2 – Les institutions européennes, une protection juridique déséquilibrée des dossiers passagers

Section 1 – Des acteurs initiateurs d’un cadre juridique favorable à la sécurité publique : le Conseil de l’Union européenne et la Commission

Section 2 – Des acteurs garants des droits fondamentaux des passagers aériens : le Parlement européen, la Cour de justice de l’Union européenne, le Comité européen de la protection des données et le Contrôleur européen de la protection des données

Partie II – Les nouvelles menaces sur la protection juridique des dossiers passagers

Titre 1 – L’affaiblissement de la protection juridique des dossiers passagers dans leur traitement aux frontières

Chapitre 1 – L’affaiblissement de la protection juridique des dossiers passagers par la collecte de données personnelles aux frontières

Section 1 – Une opération de collecte massive des données personnelles des passagers aériens

Section 2 – Un profilage des passagers aériens en conflit avec le droit à la vie privée et la protection des données personnelles

Chapitre 2 – L’affaiblissement de la protection juridique des dossiers passagers par le rôle des acteurs privés dans les aéroports

Section 1 – L’ingérence contestée des acteurs privés dans le traitement des dossiers passagers aux frontières

Section 2 – La mise en danger de la protection juridique des dossiers passagers par la privatisation des aéroports

Titre 2 – L’affaiblissement de la protection juridique des dossiers passagers par la déterritorialisation

Chapitre 1 – Une déterritorialisation par le caractère supranational des dossiers passagers : l’effacement du droit national dans les transferts de données personnelles

Section 1 – Le transfert des dossiers passagers : l’extension de l’extraterritorialité au détriment d’un espace protecteur des droits des passagers

Section 2 – Le stockage des dossiers passagers : une fragile limitation temporelle au profit de la conservation des données personnelles des passagers aériens

Chapitre 2 – Une déterritorialisation limitée par l’implication des États dans les crises contemporaines : le retour du droit national dans l’utilisation des données personnelles

Section 1 – Vers une probable extension par les États du champ d’application des dossiers passagers à la santé : une conséquence de la crise du coronavirus

Section 2 – Vers une harmonisation difficile du régime national des dossiers passagers : une conséquence de la crise du multilatéralisme

Principaux acronymes et sigles

ACLU	American Civil Liberties Union
API	Advanced Passenger Information
ASFC	Agence des services frontaliers du Canada
BEA	Bureau d'Enquêtes et d'Analyses
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
CAPPS	Computer-Assisted Passenger Prescreening System
CBP	Customs and Border Protection
CECA	Communauté Economique du Charbon et de l'Acier
CEDH	Convention Européenne des Droits de l'Homme
CEDH	Cour Européenne des Droits de l'Homme
CEPD	Comité Européen de la Protection des Données
CFAA	Computer Fraud and Abuse Act
CIL	Correspondant Informatique et Libertés
CJUE	Cour de Justice de l'Union européenne
CNIL	Commission Nationale de l'Informatique et des Libertés
COPPA	Children's Online Privacy Protection Act
CCPA	California Consumer Privacy Act
CNDP	Commission Nationale de Protection des Données Personnelles
CRS	Computer Reservation System
CTA	Certification de Transport Aérien
CVE	Countering Violent Extremism
DCS	Departure Control System
DDHC	Déclaration des Droits de l'Homme et du Citoyen
DFIC	Dubai International Financial Centre
DGAC	Direction Générale de l'Aviation Civile
DHS	Department of Homeland Security
DPF	Data Privacy Framework
DPRC	Data Protection Review Court
DPO	Data Protection Officer

ESLJ	Espace de Sécurité, de Liberté et de Justice
ESS	Système d'Entrée et de Sortie
ESTA	Electronic System for Travel Authorization
ETIAS	Système Européen d'Information et d'Autorisation concernant les Voyages
FAI	Fournisseur d'Accès Internet
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FTC	Federal Trade Commission
GCTF	Global Counterterrorism Forum
GCERF	Global Community Engagement and Resilience Fund
GLBA	Gramm-Leach-Bliley Act
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
IATA	International Air Transport Association
IPV/DP	Données Relatives aux Informations Préalables sur les Voyageurs et aux Dossiers Passagers
JAI	Justice et Affaires Intérieures
GSM	Global System for Mobile Communications
MICAS	Mesures Individuelles de Contrôle Administratif et de Surveillance
NASA	National Aeronautics and Space Administration
NPRM	Notice of Proposed Rulemaking
NSA	National Service Agency
OACI	International Civil Aviation Organization
OIV	Opérateurs d'Importance Vitale
OMD	Organisation Mondiale des Douanes
OSI	Other Service Relative Information
PCLOB	Privacy and Civil Liberties Oversight Board
PESC	Politique Étrangère et de Sécurité Commune
PIF	Point d'Accès Filtrage
PIN	Personal Identification Number

PNR	Passenger Name Record
QPC	Question Prioritaire de Constitutionnalité
RGPD	Règlement Général sur la Protection des Données
RICO	Racketeer Influenced and Corrupt Organizations
RPCV	Renseignements Préalables Concernant les Voyageurs
SAFARI	Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus
SIS	Système d'Information Schengen
SIS	Secret Intelligence Service
SLIT	Loi renforçant la Sécurité Intérieure et la Lutte contre le Terrorisme
SSI	Special Service Information
SSR	Special Service Request
STAD	Système de Traitement Automatique de Données
STIC	Système de Traitement des Infractions Constatées
SWIFT	Accord sur le Transfert de Données de Messagerie Financière de l'Union Européenne vers les États-Unis aux Fins du Programme de Surveillance du Financement du Terrorisme.
TECE	Traité Établissant une Constitution pour l'Europe
TFUE	Traité pour le Fonctionnement de l'Union Européenne
TPI	Transport Public Illicite
TUE	Traité sur l'Union Européenne
TSA	Transportation Security Administration
TWA	Trans World Airlines
UE	Union Européenne
UIP	Unité Information Passagers
URL	Uniform Resource Locator
VIS	Système d'Information sur les Visas
WCO	World Customs Organization

« Dans cinq minutes, les postes de TSF auront alerté les escales. Sur quinze mille kilomètres le frémissement de la vie aura résolu tous les problèmes. Déjà, un chant d'orgue monte : l'avion. »

Antoine de Saint-Exupéry, Vol de nuit, Gallimard, 1931

« Dirigées contre les anarchistes, les lois scélérates ont eu pour résultat de mettre en péril les libertés élémentaires de tous les citoyens. »

Léon Blum, La Revue Blanche, 1899

INTRODUCTION GÉNÉRALE

« J'avais vu des photographies de sa structure en forme d'oiseau, mais aucune ne lui rendait justice. L'intérieur était une surface continue de béton coulé. Aucune arête tranchante, aucun angle droit, aucun plafond bas et terne [...]. Par endroits les murs semblaient fondre jusqu'au sol, à d'autres ils faisaient mine de s'enrouler au-dessus de nos têtes comme des vagues sur le point de se briser [...]. Entre les voûtes, des percées de verre permettaient d'apercevoir l'empennage d'un avion ou un nuage »¹. Ces lignes, extraites du livre² du journaliste Alastair Gordon, évoquent avec ferveur le terminal TWA de l'aéroport JFK de New York, symbole de la prospérité de la métropole américaine incarnant une ville dynamique et ouverte sur le monde. Ce terminal a été fermé³ après les attentats du 11 septembre 2001, car il ne répondait plus aux normes de sécurité ; il est cependant encore aujourd'hui considéré comme un lieu doté d'un intérêt historique.

L'aéroport offre souvent la première impression d'un pays ou d'une ville pour leurs visiteurs. Il symbolise des possibilités de découvertes, de nouvelles expériences, ou d'horizons inédits pour l'arrivant. Il peut être aussi associé à l'idée de liberté et constituer le point de départ de voyages personnels ou professionnels ; représenter un moment de rupture, de découverte d'un nouvel espace, d'expérience inédite. Les premières infrastructures aéroportuaires ont vu le jour après la Première guerre mondiale⁴, lorsque le développement de l'aviation civile commençait à dessiner les contours d'un nouveau monde.

Les premiers passagers viendront dans les années 1930⁵, mus par la nécessité de voyager pour l'administration des colonies, la diplomatie, ou encore le commerce international. Tout d'abord emprunté par un nombre réduit de privilégiés, le transport aérien international échappa à la massification jusque dans les années 1960⁶. Il s'agissait d'un service de luxe dont profitait une élite qui adhérait à l'idée de courir le risque d'un voyage incontestablement

¹ C. COCHARD, « Les aéroports, ces cités des nuages », *Le Temps*, 10 juin 2023, en ligne à URL : <https://www.letemps.ch/societe/aeroports-cites-nuages> consulté le 30 août 2023

² A. GORDON, *Naked airport: a cultural history of the world's most revolutionary structure*, University of Chicago Press, 1 juin 2008.

³ A. VILLARREAL, “ Iconic TWA Flight Center Open to the Public for What May Be the Last Time ”, *Observer*, 10 octobre 2014, en ligne à URL : <https://observer.com/2014/10/twa-flight-center-open-to-the-public-for-what-may-be-the-last-time/> consulté le 30 août 2023.

⁴ C. COCHARD, « Les aéroports, ces cités des nuages », *Le Temps*, 10 juin 2023, en ligne à URL : <https://www.letemps.ch/societe/aeroports-cites-nuages> consulté le 30 août 2023

⁵ O. CACHARD, *Le transport international aérien de passagers*, Académie de droit international de La Haye, 2015.

⁶ Ibidem

aventureux. Le transport aérien a ensuite été façonné par le progrès technique. En effet, avancées dans le domaine de l'aérodynamique et les évolutions de la motorisation ont permis d'améliorer la capacité de transport des avions⁷. L'invention du réacteur et de la combustion interne ont constitué, à cet égard, un tournant décisif dans la seconde moitié du XX^e siècle. Les progrès de l'électronique ont aussi joué un rôle décisif dans le développement du secteur du transport aérien⁸. Cela a notamment permis la massification des réservations et, par conséquent, du trafic des avions. La question des données des passagers aériens a alors commencé à prendre toute son importance.

Les décennies suivantes ont été marquées par la croissance rapide de l'aviation commerciale et la multiplication des aéroports. Les stratégies en matière de marketing ont considéré que la ressource la plus rentable pour le système aéroportuaire résidait dans l'élaboration de nouvelles étapes dans le parcours des voyageurs, en s'assurant que ces derniers pouvaient profiter de nouveaux services dans les zones de transit. Dans les années 1990, le temps d'attente moyen pour un vol international était de 2 heures et 33 minutes ; l'atrium de l'aéroport est donc devenu un lieu de rassemblement pour diverses entreprises et boutiques offrant une gamme élargie et diverse de produits et services, allant des marchandises de luxe à la restauration rapide⁹. La philosophie sous-tendant le commerce dans les aéroports a ensuite évolué partout dans le monde, après les attentats du 11 septembre 2001 qui ont eu lieu aux États-Unis, avec un renforcement des mesures de sécurité et la reconfiguration des zones de circulation. Ce changement s'est notamment manifesté par l'adaptation des réglementations en vue de répondre à de nouveaux enjeux sécuritaires tout en cherchant à équilibrer les intérêts des entreprises et des voyageurs avec les exigences de sécurité.

Au fil des ans, les aéroports sont devenus des hubs permettant de multiples liaisons internationales en facilitant la mobilité des personnes et des marchandises à travers le monde. Ainsi, ils incarnent une interconnectivité croissante entre les nations, les cultures et les économies et symbolisent la globalisation qui caractérise l'époque actuelle. Aussi, ces lieux jouent un rôle crucial quant au commerce international¹⁰ : en facilitant le transport de biens et de marchandises, ils participent de la prospérité économique en permettant la concrétisation des affaires et l'expansion des échanges dans le monde. Ces plateformes sont aussi des

⁷ Ibidem

⁸ Ibid.

⁹ C. COCHARD, « Les aéroports, ces cités des nuages », *Le Temps*, 10 juin 2023, en ligne à URL : <https://www.letemps.ch/societe/aeroports-cites-nuages> consulté le 30 août 2023.

¹⁰ C. HALPERN, D. LORRAIN, « HUB (aéroports et ports) », *Flux*, 2010/1-2, N°79-80, p. 140 à 152, 2010, en ligne à URL : <https://www.cairn.info/revue-flux1-2010-1-page-140.htm?contenu=article> consulté le 30 août 2023

endroits où les différentes cultures se croisent, reflétant toute la richesse de la diversité du monde : les voyageurs en provenance de différents pays se rassemblent dans les aéroports, faisant de ce lieu le symbole d'un environnement multiculturel où interagissent les peuples.

Par ailleurs, le secteur du transport aérien est particulièrement propice à l'utilisation de nouvelles technologies et à l'innovation. Il a ainsi pris une avance significative en matière d'automatisation, aussi bien au sol qu'à bord. L'apparition de certaines technologies de collecte de données dans les aéroports a contribué à la transformation du secteur aérien¹¹. Cela s'est notamment traduit par une automatisation accrue de différents services comme la maintenance ou la sécurité. La pandémie du Covid-19 a accéléré un mouvement d'automatisation mondiale avec le développement des services liés à l'enregistrement et au guidage des passagers¹². La numérisation et les automates ont été privilégiés pour limiter les contacts humains, donc la propagation du virus, au sein des aéroports. Dans le même temps, les systèmes de reconnaissance faciale, de vérification de bagages et de fouilles à distance se sont développés¹³. Cette automatisation avait pour but de fluidifier les flux des passagers et ainsi de réduire le temps de passage dans les aéronefs. Cette évolution a mis en valeur le rôle grandissant des données à caractère personnel dans le secteur aéroportuaire.

À cet égard, l'entrepreneur britannique Clive Humby a comparé, en 2006, les données personnelles au pétrole : « les données sont le nouveau pétrole. Elles sont précieuses, mais si elles sont brutes, elles sont inutiles. Vous devez les raffiner pour les transformer en carburant »¹⁴. C'est de cette analogie que viendrait l'expression envisageant les données personnelles comme constituant « l'or noir du XXI^e siècle »¹⁵. Ce rapprochement fait allusion à la valeur économique croissante que ces données ont acquise dans le contexte numérique des vingt dernières années. Le pétrole est en effet traditionnellement considéré comme l'une des ressources les plus précieuses et influentes dans le monde. Plusieurs raisons expliquent une telle comparaison des données personnelles à l'or noir.

¹¹ Direction générale de l'Aviation civile, *Activités liées aux aéroports à l'horizon 2025*, Les notes d'analyse de la DGAC, Eclairages, Septembre 2017, n°3, en ligne à URL : https://www.ecologie.gouv.fr/sites/default/files/Eclairage_n_3_VF_web.pdf consulté le 29 août 2023.

¹² Académie de l'Air et de l'Espace, *Automatisation des avions de transport à l'horizon 2050*, Étude, Aviation plus automatique, interconnectée, à l'horizon 2050, Commission aéronautique civile, Dossier N°42, 2018, en ligne à URL : <https://academieairespace.com/wp-content/uploads/2018/07/Les-Livrets-Web.pdf> consulté le 29 août 2023.

¹³ R. FLÉCHAUX, « L'observabilité pour assurer la fluidité du trafic à l'aéroport de Rome », *Le Monde Informatique*, 28 août 2023, en ligne à URL : <https://www.lemondeinformatique.fr/actualites/lireamp-l-observabilite-pour-assurer-la-fluidite-du-traffic-a-l-aeroport-de-rome-91369.html> consulté le 29 août 2023.

¹⁴ M. PALMER, "Data is the new oil!", ANA Marketing Maestros, 2006, en ligne à URL : https://ana.blogs.com/maestros/2006/11/data_is_the_new.html consulté le 27 août 2023.

¹⁵ M. KERSHNER, "Data isn't the new oil – Time is", *Forbes*, 15 juillet 2021, en ligne à URL : <https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/> consulté le 27 août 2023.

Une première est que les données personnelles ont une valeur économique. En effet, parce qu'elles permettent de connaître les habitudes, les comportements ainsi que les préférences des individus, notamment en matière de consommation, ces données, très recherchées, sont devenues une arme précieuse sur un marché à forte concurrence¹⁶. Dès lors qu'elles sont en possession de ces données, les entreprises qui les traitent peuvent s'adapter aux tendances de consommation en proposant des offres, produits et services personnalisés. Or, l'adaptation de leur stratégie marketing peut se traduire par des gains économiques importants.

Ainsi, les entreprises qui détiennent une importante quantité de données personnelles possèdent un avantage compétitif sur les autres, à la manière des pays possédant des réserves de pétrole et qui en font un levier d'influence politique et économique¹⁷. Ces données personnelles se présentent donc comme un outil économique significatif. Leur utilisation dépasse donc la problématique sécuritaire étant donné qu'elles peuvent être employées pour d'autres finalités : influencer les marchés et les décisions politiques ou réorienter les influences culturelles en place. Toutefois, pour avoir une valeur réelle significative, les données collectées doivent d'abord être traitées et analysées afin d'en extraire tout leur intérêt, à l'image du pétrole¹⁸ qui doit être raffiné et transformé pour devenir un produit fini après extraction. Dès lors, les entreprises technologiques sont indispensables pour collecter, agréer et analyser ces données afin d'en tirer un maximum d'informations exploitables.

Cette comparaison n'est pas exempte d'inconvénients. L'industrie pétrolière a souvent fait l'objet de controverses liées au respect de l'environnement, à l'éthique et aux droits de l'Homme¹⁹. De même, la collecte massive et l'utilisation de données personnelles soulèvent des défis vis-à-vis du respect de la vie privée, de la protection des données à caractère personnel et des droits fondamentaux. Les législateurs, notamment au sein de l'Union européenne (UE), tentent de mettre en place des cadres juridiques pour protéger les droits des utilisateurs tout en permettant une utilisation responsable des données. Cet encadrement normatif est devenu un enjeu politique car l'accumulation de données personnelles par quelques grandes entreprises crée un déséquilibre de pouvoir similaire à celui observé avec le pétrole. Cette situation peut entraîner des inquiétudes pour les sociétés, notamment quant à une domination économique et une surveillance généralisée.

¹⁶ B. CASSAR, *Données – gouvernance des données*, Dalloz, Répertoire IP/IT et Communication, mars 2022.

¹⁷ C. FERAL-SCHUHL, *Données en matière pénale*, Dalloz, Praxis Cyberdroit, Chapitre 134, 2021.

¹⁸ J. KREWER, « La donnée est-elle le nouveau pétrole ou un nouvel environnement ? », *Usbek & Rica*, 9 mai 2018, en ligne à URL : <https://usbeketrica.com/fr/article/quatre-metaphores-pour-une-politique-de-la-donne> consulté le 28 août 2023.

¹⁹ M. TSAYEM DEMAZE, « Quête de justice climatique et reconfiguration de la lutte contre les changements climatiques en marge des COP », *L'Information géographique*, vol. 87, n° 3, 2023, pp. 25-47.

Toutefois, malgré ces similitudes, les données à caractère personnel et le pétrole sont deux ressources très différentes. Les données sont des informations liées à la vie privée et à l'identité des individus, une nature qui soulève des questions éthiques et juridiques uniques. Comparer ces données à l'or noir permet de mettre en évidence leur importance économique mais ne doit pas occulter les préoccupations relatives à la vie privée et à la sécurité.

Section 1 – L'intérêt accru du secteur du transport aérien pour les données personnelles

Le secteur du transport aérien s'est de plus en plus intéressé aux données personnelles des passagers pour diverses raisons liées à la sécurité, à la gestion des voyageurs, à l'encadrement juridique et à la protection de ces données. Celles-ci sont intéressantes pour le secteur du transport aérien, sous différents angles. Le transport aérien de passagers est défini comme le déplacement d'une personne physique, d'un point à un autre, à bord d'un aéronef d'après les prévisions d'un contrat²⁰. Juridiquement, le transport aérien de passagers est encadré par les conventions internationales²¹. Les codes nationaux régissent l'aviation civile pour les transports internes²². Jadis réservé à une élite, le transport aérien de passagers s'est aujourd'hui démocratisé à travers notamment la commercialisation de vols. Avec une moyenne de plus de 100 000 vols par jour à travers le monde²³, chiffre multiplié par deux en haute saison, le transport aérien n'est plus aujourd'hui qu'un article parmi d'autres de la société de consommation contemporaine qui n'est pas dénué de conséquences négatives, en particulier en matière de changement climatique²⁴.

Dans le cadre de la lutte contre le terrorisme et les crimes graves, les compagnies aériennes et les autorités publiques portent un intérêt fondamental à la sécurité des passagers et, plus généralement au transport aérien. La collecte et l'analyse de données personnelles, comme les

²⁰ O. CACHARD, *Le transport international aérien de passagers*, Académie de droit international de La Haye, 2015.

²¹ On peut citer la Convention de Varsovie, pour l'unification de certaines règles relatives au transport aérien international, signée en 1929 et remplacée par la Convention de Montréal en 1999. Il y a également la Convention de Chicago, relative à l'aviation civile internationale, qui a instauré en 1944 l'Organisation de l'aviation civile internationale. Cette agence spécialisée des Nations-Unies est chargée de la coordination et de la régulation du transport aérien international.

²² En France, le code des transports, promulgué en 2010, regroupe les dispositions juridiques relatives aux transports en France. Les dispositions législatives encadrant les données des passagers aériens en France, sont au code de la sécurité intérieure.

²³ J-L DELMAS, « Aviation : Combien d'avions pourrait-on avoir au maximum dans le ciel avant qu'il ne soit saturé ? », *20 Minutes*, 21 juin 2023, en ligne à URL : <https://www.20minutes.fr/economie/4042146-20230621-aviation-combien-pourrait-avoir-maximum-ciel-avant-sature#:~:text=Selon%20le%20Groupe%20d'action,m%C3%A4me%20%C3%A4tre%20multipli%C3%A9%20par%20deux> consulté le 24 août 2023.

²⁴ Parlement européen, « Émissions de CO2 des avions et des navires : faits et chiffres (infographie) », *Société*, 14 juin 2022, en ligne à URL : <https://www.europarl.europa.eu/news/fr/headlines/society/20191129STO67756/emissions-de-co2-des-avions-et-des-navires-faits-et-chiffres-infographie> consulté le 28 août 2023.

noms, les dates de naissance, les itinéraires de voyage et d'autres informations propres aux passagers permettent d'identifier des menaces potentielles et de prévenir des activités terroristes²⁵. Ces données personnelles sont utilisées lors du contrôle aux frontières et permettent de garantir que les passagers détiennent les documents nécessaires pour entrer dans un pays. Cela peut inclure des données biométriques²⁶ comme les empreintes digitales et des photographies pour confirmer l'identité des passagers.

En outre, ces données sont utilisées pour la gestion des réservations, l'enregistrement des passagers, la distribution des sièges et d'autres aspects opérationnels du transport aérien. Elles ont alors pour objectif de contribuer à rendre le processus de voyage plus efficace et fluide²⁷. Les compagnies aériennes utilisent également ces données pour personnaliser les services offerts aux passagers. Cela peut inclure des recommandations de destinations, des offres spéciales et d'autres avantages en accord avec les préférences individuelles du consommateur et voyageur.

Toutefois, les législations et accords encadrant l'aviation civile exigent souvent que les compagnies aériennes protègent les données à caractère personnel de leurs passagers²⁸ et les utilisent de manière responsable. Cela implique le respect des lois sur la protection de la vie privée et la mise en place de mesures de sécurité informatique pour éviter les violations de données. En cas de perturbations de vol, les données personnelles sont utilisées pour identifier les passagers concernés et faciliter le processus de compensation ou d'indemnisation. De plus, en période de pandémies, les données personnelles peuvent être utilisées pour suivre les flux de passagers et prendre les bonnes mesures de santé publique, comme la mise en quarantaine.

Au sein de l'Union européenne, la principale législation qui régit la protection des données personnelles est le Règlement Général sur la Protection des Données (RGPD)²⁹. Ce règlement, entré en vigueur le 25 mai 2018, a eu un impact sur la collecte, le traitement et l'utilisation des données personnelles, y compris dans le contexte des services personnalisés

²⁵ Conseil européen, « Les systèmes informatiques pour lutter contre la criminalité et sécuriser les frontières de l'UE », *Europa*, Politiques, 13 mars 2023, en ligne à URL : <https://www.consilium.europa.eu/fr/policies/it-systems-security-justice/> consulté le 29 août 2023.

²⁶ Ibidem

²⁷ Organisation de l'aviation civile internationale, « Le rôle du voyage fluide et sans contact dans la relance du transport aérien au cœur de l'édition 2021 du Symposium TRIP », *Communiqué*, Montréal, 26 mai 2021, en ligne à URL : <https://www.icao.int/Newsroom/NewsDoc2021fix/COM.36.21.FR.pdf> 29 août 2023.

²⁸ Ligue des droits de l'Homme, *Protection des données personnelles*, Analyse comparée des législations et des pratiques dans neuf pays européens dans le contexte du cadre juridique européen, juin 2010, en ligne à URL : <https://www.ldh-france.org/wp-content/uploads/IMG/pdf/SynthesfrancaisFINALcorr-BD.pdf> consulté le 29 août 2023.

²⁹ 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).

offerts par les compagnies aériennes. En effet, ce texte « établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données »³⁰ et « protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel »³¹. De ce règlement découlent donc un certain nombre de droits.

Les voyageurs ont tout d'abord le droit d'être informés de la manière dont leurs données personnelles sont collectées, traitées et utilisées. Les compagnies aériennes doivent en ce sens fournir des informations compréhensibles et claires sur leurs pratiques de personnalisation des services dans les aéroports (droit d'information)³². Les passagers ont aussi le droit d'accéder aux données que les compagnies aériennes détiennent à leur sujet et de demander des corrections si celles-ci, utilisées pour personnaliser leurs services, sont incorrectes (droit d'accès et de rectification)³³. Les utilisateurs des transports aériens bénéficient également du droit de demander la suppression de leurs données personnelles si elles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées. C'est le cas, par exemple, d'un passager qui ne souhaite plus que ses données soient utilisées pour personnaliser tel ou tel services (droit à l'effacement)³⁴. Aussi, certaines données sont considérées comme sensibles, c'est le cas pour les données médicales ou religieuses. Le traitement de telles données est soumis à un régime plus strict selon le règlement européen précité (interdiction du traitement des données sensibles)³⁵.

Conséquemment, les compagnies aériennes opérant en France, et plus largement dans l'Union européenne, et offrant des services personnalisés doivent se conformer aux exigences du RGPD lorsqu'elles collectent et utilisent des données personnelles à des fins de personnalisation. D'autres règles européennes spéciales ont été élaborées pour encadrer les données personnelles qui sont utilisées pour des visées particulières, comme la lutte contre le terrorisme³⁶.

³⁰ Article premier, RGPD.

³¹ Ibidem

³² Article 13 à 15, RGPD.

³³ Article 16, RGPD.

³⁴ Article 17, RGPD.

³⁵ Article 9, RGPD.

³⁶ 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. Lire en ce sens P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue Française de droit aérien et spatial*, Vol. 278, n° 2, 2016.

Section 2 – Les dossiers passagers, un outil de lutte contre les infractions terroristes et transnationales

« Le PNR sera un outil précieux pour renforcer la sécurité des citoyens européens en facilitant en amont le repérage des mouvements des terroristes djihadistes qui empruntent les transports aériens à la fois à travers l'Europe, mais aussi entre l'Europe et les autres régions du monde, pour les empêcher de passer à l'acte ». Cette phrase est tirée du communiqué de presse³⁷ du ministre de l'Intérieur français, en date du 14 avril 2016, qui saluait l'adoption par le Parlement européen de la directive Passenger Name Record (PNR)³⁸. Ce texte prévoit notamment le transfert, par les transporteurs aériens, de données des dossiers passagers (PNR) de vols extra-UE et le traitement de ces données, notamment leur collecte, leur utilisation et leur conservation par les États membres ainsi que leur échange entre États membres³⁹. La directive prévoit également que ces données des dossiers passagers ne sont traitées qu'à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité ainsi que d'enquêtes et de poursuites en la matière⁴⁰.

Le terme de passager aérien n'est pas explicitement défini ni par le droit international ni par le droit de l'Union européenne. Toutefois, le juriste Olivier Cachard définit le passager aérien comme « une personne physique qui, hors les cas d'apatridie, est liée à un ou plusieurs États par une nationalité »⁴¹. Cette dernière lui permet d'entrer ou de sortir d'un territoire ; elle peut également l'empêcher d'entrer dans un autre pays. De cette nationalité – et de la localisation de son domicile – découlent des droits dont l'État est garant. Le passager est aussi celui qui voyage au moyen d'un titre d'un titre de transport, qu'il obtient à titre onéreux.

Les données PNR sont des fichiers créés par les compagnies aériennes pour chaque voyage réservé par un passager⁴² stockés sur les bases de données de réservation et de contrôle des départs de ces compagnies. Ils permettent à tous les intervenants du secteur aérien de connaître chaque passager et d'avoir accès à toutes les informations pertinentes concernant

³⁷ B. CAZENEUVE, « La directive Passenger Name Record (PNR) a été adoptée par le Parlement européen le 14 avril 2016 », *Ministre de l'intérieur*, Communiqué de presse, 14 avril 2016, en ligne à URL : <https://www.interieur.gouv.fr/Archives/Archives-des-communiqués-de-presse/2016-Communiqués/Adoption-du-PNR-par-le-Parlement-europeen> consulté le 23 août 2023.

³⁸ 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.

³⁹ L'objet et le champ d'application de la directive sont précisés à l'article premier de la directive. Directive (UE) PNR, Article 1, alinéa 1.

⁴⁰ Directive (UE) PNR, Article 1, alinéa 2.

⁴¹ O. CACHARD, *Le transport international aérien de passagers*, Académie de droit international de La Haye, 2015.

⁴² Y. MAYAUD, *Répertoire de droit pénal et de procédure pénale*, Dalloz, Terrorisme – Prévention, janvier 2018.

son voyage. Ces données PNR se distinguent des données API (Advanced Passenger Information) qui recouvrent les données biographiques recueillies sur le passager par les compagnies aériennes lors de la phase d'enregistrement sur un vol. Cette deuxième catégorie de données se concentre davantage sur les caractéristiques du vol que sur le profil du passager⁴³. Une troisième catégorie de données est parfois mentionnée, ce sont les Renseignements préalables concernant les voyageurs (RPCV) qui couvrent des informations générales sur le vol ainsi que l'identification des passagers et des membres de l'équipage. Plus fournies que les autres fichiers de données, les données PNR enregistrées lors de la réservation du titre transport prennent la forme d'enregistrements standardisés sur le plan international et contiennent des informations sur le vol, le passager, l'agent de voyage sollicité, le moyen de paiement utilisé, le numéro de siège, la nature de bagages et d'autres catégories d'informations.

Avant les attaques terroristes du 11 septembre 2001, les données des dossiers passagers avaient surtout un aspect commercial puisqu'elles étaient fournies par les voyageurs au stade de la réservation commerciale et utilisées par les transporteurs aériens dans leurs systèmes de billetterie, de réservation et d'enregistrement pour suivre le trajet du passager. Toutefois, elles pouvaient être requises par les autorités judiciaires pour les besoins d'une enquête ou d'une instruction. À cette époque, aucune législation n'avait prévu un régime spécifique selon lequel les transporteurs et les agences de voyages étaient obligés de transmettre ces données aux autorités compétentes à des fins de répression des infractions dans le secteur de l'aviation civile. Ce n'est qu'après cet acte terroriste sur le sol américain qu'elles se sont transformées en outil de lutte contre le terrorisme et le crime organisé⁴⁴.

L'intervention du ministre de l'Intérieur français sur les données PNR, évoquée ci-dessus, n'est pas anodine puisque la France a été l'un des États membres de l'Union européenne qui a encouragé l'adoption de cette directive en tant qu'instrument de lutte contre le terrorisme et la criminalité transnationale ; celle-ci ayant été l'un des pays les plus touchés par des attaques terroristes et par le retour de combattants terroristes les années précédant l'adoption de ce texte européen⁴⁵. La directive PNR a pour but la mise en place d'une coopération entre États

⁴³ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, Vol. 278, n°2, 2016.

⁴⁴ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019. Lire également. Sénat, Commission des lois, Rapport N°401 : *La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives*, présenté par M. Simon Sutour et M. Yves Détraigne, 13 mai 2009.

⁴⁵ Gouvernement, « Adoption du PNR par le Parlement européen », *Communiqué*, 14 avril 2016, en ligne à URL : <https://www.gouvernement.fr/partage/6939-adoption-du-pnr-par-le-parlement-europeen> consulté le 24 août 2023.

membres permettant l'échange et l'exploitation de ce type de données, tout en respectant les libertés publiques. Cette législation ne crée pas de dispositif PNR européen *stricto sensu*, tel qu'un seul fichier de données centralisé, mais les conditions d'un début de coordination entre les vingt-sept systèmes PNR déjà existants ou à créer. L'objectif pour le législateur européen est d'encadrer les règles des États membres relatives aux obligations des transporteurs aériens en matière de transmission des données et de définir des modalités communes de traitement de celles-ci⁴⁶.

Dès 2014, la France avait mis en place son propre système PNR pour la collecte des données des dossiers passagers, qu'elle a utilisé à titre expérimental jusqu'au 31 décembre 2017. Le système a été institué pour les besoins de la « prévention et de la constatation des actes de terrorisme, des infractions mentionnées à l'article 695-23 du Code de procédure pénale et des atteintes aux intérêts fondamentaux de la Nation, du rassemblement des preuves de ces infractions et de ces atteintes ainsi que de la recherche de leurs auteurs ». Codifiées dans le Code de la sécurité intérieure⁴⁷, ces dispositions définissaient le contenu et les conditions d'exploitation du nouveau fichier national de données PNR.

Les activités liées au terrorisme et à la criminalité organisée ne se limitant plus au territoire national, cela implique des déplacements internationaux pour les personnes qui participent à de tels actes. Dans ce contexte d'évolution de l'activité terroriste et de la criminalité organisée, le traitement des données PNR s'avère inévitable puisqu'il peut permettre aux autorités répressives du monde entier d'identifier les individus susceptibles d'être à l'origine de ces actions, avant leur commission, alors même qu'ils ne sont pas soupçonnés d'activités terroristes ou criminelles⁴⁸. Toutefois, nous l'avons relevé pour la France, avant même que le traitement des données PNR ne se généralise dans le monde, au niveau national, la plupart des États du monde les utilisaient déjà au bénéfice des services de police et des autorités locales.

Au niveau de l'Union européenne, la directive PNR a fait l'objet de nombreux débats compte tenu du fait qu'elle implique la collecte et le traitement des données passagers, soulevant ainsi des questions relatives à la protection de la vie privée et au droit à la protection des données à

⁴⁶ 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.

⁴⁷ Article R. 232-12 du Code de la Sécurité Intérieure.

⁴⁸ Conseil européen, « Directive de l'UE relative aux données des dossiers passagers (PNR) », *Europa*, Politique, Action de l'UE face au terrorisme, 31 août 2022, en ligne à URL : <https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/passenger-name-record/#pnr> consulté le 24 août 2023.

caractère personnel⁴⁹. Ainsi, pour les partisans de la directive, celle-ci est essentielle pour renforcer la sécurité et la coopération internationale en matière de lutte contre les actes terroristes et la criminalité transnationale tandis que les critiques s'interrogent sur les risques, d'une part, de violation du droit à la protection de vie privée et des données à caractère personnel et, d'autre part, d'utilisation abusive de ces dernières. L'approbation de la directive n'a pas mis fin à ces critiques ; dès lors qu'un acte juridique sur l'utilisation des données personnelles est proposé, ces débats refont jour. Par exemple, ce fut le cas le 19 octobre 2006, lors de la signature du premier accord d'échange de données des passagers aériens entre l'Union européenne et les États-Unis⁵⁰.

Après les attentats du 11 septembre 2001, dans le cadre de la lutte contre le terrorisme et la criminalité organisée, le gouvernement américain avait adopté, le 19 novembre 2001, une loi sur la sécurité de l'aviation et du transport (the Aviation and Transportation Security Act). Puis, le 5 mai 2002, une autre loi renforçant les conditions d'entrée sur le territoire américain (Enhanced Border Security and Visa Entry Reform Act) a également été votée. Ces mesures disposaient qu'à compter du 5 mars 2003, les compagnies aériennes devaient communiquer aux services des douanes et de la sécurité américains des informations personnelles relatives à leurs passagers, sous peine de contrôles renforcés, d'amendes ou même de suspension du droit d'atterrir⁵¹.

Section 3 – Les données personnelles des dossiers passagers, sujet de frictions entre deux libertés fondamentales

Ces lois américaines ont posé des défis aux Européens car elles heurtaient les règles européennes en matière de protection des données à caractère personnel. La conclusion d'un accord entre l'Union européenne et les États-Unis était en fait nécessaire⁵² afin que les compagnies aériennes ne soient pas placées en porte-à-faux entre les législations américaines et européennes. Un accord a ainsi été conclu le 19 octobre 2006 et est entré en vigueur le 1^{er} août 2007. Un second texte a été adopté fin juillet 2017, renégocié à partir de la fin de l'année

⁴⁹ Ibidem

⁵⁰ Parlement européen, *Résolution du Parlement européen du 12 juillet 2007 sur l'accord avec les États-Unis d'Amérique concernant l'utilisation de données des dossiers des passagers aériens (PNR)*, 12 juillet 2007. Cette résolution revient sur l'accord entre la Communauté européenne et les États-Unis le 19 octobre 2006.

⁵¹ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019. Lire également. P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue Française de droit aérien et spatial*, Vol. 278, n° 2, 2016.

⁵² S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019. Lire également. F. MARIATTE, « Protection des données personnelles des usagers des transports aériens », *Nouvelles technologies*, Europe, LexisNexis, n° 7, juillet 2004.

2010. Validé par le Parlement européen et le Conseil de l'Union européenne en avril 2012, un nouvel accord est entré en vigueur le 1^{er} juillet 2012 pour une durée de sept ans. A alors débuté un débat incessant entre sécurité collective et libertés individuelles, en ce qui concerne les données PNR, qui tourne autour de l'équilibre délicat à trouver entre la nécessité de garantir la sécurité publique et la protection des droits fondamentaux des individus tels que la vie privée et le respect des données à caractère personnel.

Des points récurrents ont été soulevés afin d'assurer une meilleure protection juridique des dossiers passagers⁵³ dont l'interdiction de la collecte et de l'utilisation de données sensibles, la limite de la durée de leur conservation, en général de cinq ans, la mise en place d'une unité d'informations chargée de la gestion de la protection desdites données, le droit d'information des passagers sur la collecte de leurs données et leurs droits à cet égard, l'interdiction du profilage, le transfert à des pays tiers dans le cadre de l'Union européenne et ses limites. Les débats autour de ces questions visent à consolider la garantie des droits fondamentaux en matière de protection des données à caractère personnel, de droit au respect de la vie, de droit à la non-discrimination ; ceci justifiant ces types de restrictions à l'utilisation et au transfert des données PNR.

Ainsi, pour le législateur européen, l'utilisation des données PNR, notamment la confrontation de celles-ci à diverses bases de données de personnes recherchées, est « nécessaire »⁵⁴ en vue de la prévention et la détection des infractions terroristes et crimes transnationaux ainsi que pour permettre des enquêtes et des poursuites en la matière. Elle permettrait un renforcement de la sécurité intérieure dans l'objectif de rassembler des preuves et, le cas échéant, pour identifier et appréhender les complices de crimes ainsi que démanteler les réseaux criminels. Prévenir le terrorisme et les formes graves de criminalité constituent l'un des objectifs de l'utilisation des données des dossiers passagers, d'où le besoin d'une « évaluation »⁵⁵ préalable de ces données afin d'identifier les individus qui n'étaient pas soupçonnés de participation à ces infractions mais qui devraient être soumis à un examen davantage approfondi par les autorités du pays concerné.

L'utilisation des données des dossiers passagers permet en conséquence de lutter contre la menace que représentent les infractions terroristes et les formes graves de criminalité d'une

⁵³ V.CORREIA, « Fasc. 978 : Données Des Passagers Aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

⁵⁴ 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.

⁵⁵ Ibidem

manière différente que celle employée pour d'autres catégories de données à caractère personnel. Toutefois, là encore, le législateur européen et les parties prenantes aux accords PNR bilatéraux, tel que l'accord euro-américain, ont prévu des dispositions pour limiter le traitement de telles données au nécessaire⁵⁶. Le débat autour du sujet étudié porte principalement sur le fait de savoir si ces limitations sont effectives ou si la balance entre sécurité collective et protection des droits fondamentaux penche en faveur de la première.

Cette discussion sur les données PNR est en effet fondamentalement une question d'équilibre entre la sécurité collective et la protection des droits individuels. Trouver un compromis entre ces deux préoccupations est un défi complexe pour les législateurs et les gouvernants. La collecte de données PNR implique une vaste récolte d'informations personnelles sur les passagers telles que les itinéraires de voyage, les coordonnées de contact, les informations de paiement, etc. Les défenseurs de l'utilisation des données des dossiers passagers soutiennent que celles-ci sont essentielles pour identifier les individus impliqués dans des activités criminelles, y compris le terrorisme. Cependant, les critiques⁵⁷ du système soulignent que cela peut constituer une intrusion majeure dans la vie privée des passagers, car leurs déplacements et leurs habitudes peuvent ainsi être étroitement surveillés. La manière dont les données PNR sont utilisées est également un point de discorde. Les partisans de l'utilisation des données PNR pour des visées sécuritaires⁵⁸ font valoir qu'elles sont essentielles pour prévenir les menaces potentielles et pour enquêter sur les activités criminelles. Cependant, les opposants s'inquiètent du risque d'abus de pouvoir, de profilage illégal⁵⁹ et de conservation des données à des fins non liées à la sécurité.

Les défenseurs des libertés individuelles⁶⁰ demandent une plus grande transparence concernant la manière dont les données PNR sont collectées, stockées et partagées entre les

⁵⁶ L'article 4 de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure de 2012, prévoit l'utilisation et le traitement des dossiers passagers à « des fins de prévention et de détection des infractions » ainsi que « d'enquêtes et de poursuites » qu'il liste, incluant notamment les infractions terroristes et infractions pénales.

⁵⁷ V. MITSILEGAS, « Contrôle des étrangers, des passagers, des citoyens : surveillance et anti-terrorisme », *Cultures & conflits*, 60, 2005.

⁵⁸ F. RIVIERE, « Bernard Squarcini: 'Il faut renforcer les moyens des services de renseignement' », *RFI*, 13 février 2015, en ligne à URL : <https://www.rfi.fr/fr/emission/20150213-bernard-squarcini-invite-frederic-riviere-services-renseignements-terrorisme> consulté le 24 août 2023.

⁵⁹ J. LAGASSE, « Fichier "PNR" : surveillance électronique de masse ou nouveau paradigme de la sécurité ? », *Les Notes du CREOGN*, N° 19, 2016, en ligne à URL : <https://hal.science/hal-03096592/document> consulté le 24 août 2023.

⁶⁰ Avis du CEPD sur le mandat de négociation d'un accord entre l'UE et le Japon pour le transfert et l'utilisation de données des dossiers passagers, 6/2019, 25 octobre 2019, en ligne à URL : https://edps.europa.eu/sites/default/files/publication/19-10-25_opinion_recommandation_pnr_japan_fr.pdf consulté le 24 août 2023.

pays. Ils insistent sur la nécessité de garantir des mécanismes de contrôle et de recours pour les individus dont les données sont collectées. L'absence de transparence et de contrôle adéquat peuvent conduire à des inquiétudes quant à une surveillance généralisée et injustifiée. Certains débats portent aussi sur l'efficacité réelle du système PNR en tant qu'outil de lutte contre le terrorisme et la criminalité. L'un des directeurs centraux du renseignement intérieur français justifiait le système PNR en le présentant comme un outil efficace contre le nouveau terrorisme international⁶¹, qui ne repose plus sur un soutien étatique mais sur des individus relativement isolés qui agissent parfois en réseau. Subséquemment, l'évolution du terrorisme contemporain requiert un travail de détection précoce pour prévenir et évaluer efficacement et rapidement la dangerosité de la menace. Un tel outil permettrait alors de mieux tracer les flux potentiellement criminogènes et de neutraliser judiciairement les individus avant qu'ils n'agissent. Les données PNR pourraient ainsi être utiles lorsqu'elles fournissent un grand nombre d'indicateurs utiles qui, agrégés à d'autres données, peuvent générer de nombreux renseignements efficaces. Le haut responsable français a également souligné qu'en matière de renseignement, les données seules sont rarement décisives en elles-mêmes.

D'autres experts⁶² estiment que l'efficacité de la collecte de données PNR peut être limitée, car les individus mal intentionnés pourraient trouver des moyens de contourner ces mesures de surveillance tandis que les passagers ordinaires pourraient être soumis à une surveillance excessive sans bénéfice significatif pour la sécurité. D'autres commentateurs critiques considèrent que le dispositif PNR pose des défis pour le respect des droits fondamentaux⁶³, notamment le droit à la vie privée et à la protection des données à caractère personnel. Ils soulignent⁶⁴ que des mesures de sécurité intrusives pourraient entraîner des discriminations et des stigmatisations injustes, en particulier envers un groupe de personnes en raison de leurs orientations politiques ou religieuses. Ainsi, paradoxalement, cet endroit qu'est l'aéroport qui devait être un lieu de confort, de fluidité et de divertissement, devient de plus en plus un endroit contraignant.

Pour reprendre les mots du doyen Carbonnier : « Le droit est trop humain pour prétendre à l'absolu de la ligne droite. Sinueux, capricieux, incertain tel il nous est apparu ... Flexible

⁶¹ Sénat, Commission des lois, Rapport n°401 : *La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives*, présenté par M. Simon Sutour et M. Yves Détraigne, 13 mai 2009.

⁶² B. SCHNEIER, "Security and Function Creep", IEEE Security and Privacy Magazine, 2010.

⁶³ AFP, « Fichier des passagers : la commission européenne prête à modifier sa proposition », Vosges matin, Terrorisme, 21 janvier 2015, en ligne à URL : <https://www.vosgesmatin.fr/actualite/2015/01/21/fichier-des-passagers-la-commission-europeenne-prete-a-modifier-sa-proposition> consulté le 24 août 2023.

⁶⁴ B. VAN DER SLOOT, "Passenger Name Record", European Human Rights Cases, 2017, en ligne à URL : <https://bartvandersloot.com/onewebmedia/pnr.pdf> consulté le 24 août 2023.

droit !... Rigueur, raideur. Raide comme la justice, c'était autrefois la comparaison courante dans les milieux populaires ... Combien de générations de justiciables avaient dû d'abord se rompre les os sur la justice pour en arriver à la juger aussi brièvement. Si ce livre ne peut être une leçon, qu'il lui suffise d'être légèrement une revanche »⁶⁵. Cette citation éclaire notre réflexion quant au droit des dossiers passagers, un droit naissant qui doit être pris tel qu'il est, c'est-à-dire un droit flexible naviguant entre le souci de la sécurité publique et celui de la protection des droits fondamentaux, entre l'érosion des règles des législations et accords bilatéraux portant sur les dossiers passagers et une tentative d'harmonisation des normes en la matière. Il s'agit d'un droit qui se caractérise ainsi par sa relativité, sa diversité interne, sa vivacité, sa fluctuabilité et son influence plus ou moins forte selon les circonstances du moment⁶⁶. Sous-tendu par des considérations politiques et traitant de thèmes sensibles comme le terrorisme et le crime transnational, d'une part, la garantie du droit à la vie et la protection des données à caractère personnel, d'autre part, ce droit n'est pas exempt de tensions qui tirent les priorités du législateur d'un côté ou de l'autre, en fonction du contexte politique⁶⁷.

L'hypothèse directive de la présente étude consiste à entendre le droit des dossiers passagers comme un droit pris dans un mouvement historique, autrement dit de considérer le développement d'accords et d'actes juridiques relatifs aux données PNR suivant une perspective évolutive. « Le droit est dans le devenir, est donc devenir lui-même » écrivait encore le doyen Carbonnier⁶⁸. L'évolution du droit PNR est souvent motivée par la nécessité de renforcer les mesures de sécurité et de prévenir les actes de terrorisme. Les législations peuvent être adaptées pour permettre un partage plus efficace des données entre les compagnies aériennes et les autorités compétentes afin d'identifier plus rapidement les passagers présentant des risques potentiels. Avec un accent croissant mis sur la protection de la vie privée et des données personnelles, les règles relatives aux données PNR évoluent pour garantir que leur collecte, leur stockage et leur traitement respectent les normes de protection de la vie privée et des données à caractère personnel. Les passagers doivent être informés de la manière dont leurs données seront utilisées et donner leur consentement éclairé. Par ailleurs, les vols internationaux impliquant souvent le transfert de données PNR entre

⁶⁵ J. CARBONNIER, *Flexible droit : Pour une sociologie du droit sans rigueur*, LGDJ, Anthologie du droit, 2013.

⁶⁶ J.-J. SARFATI, « Des limites de l'idée du droit flexible », *Le Philosophoire*, 2012/2, n°38, pp. 207 à 228, 2012, en ligne à URL : <https://www.cairn.info/revue-le-philosophoire-2012-2-page-207.htm> consulté le 24 août 2023.

⁶⁷ X. DELPECH, « La directive PNR confrontée au respect des droits fondamentaux », *Dalloz*, Affaires, IP/IT et Communication, Droits fondamentaux, 19 septembre 2022, en ligne à URL : <https://www.dalloz-actualite.fr/flash/directive-pnr-confrontee-au-respect-des-droits-fondamentaux> consulté le 24 août 2023.

⁶⁸ J. CARBONNIER, *Flexible droit : Pour une sociologie du droit sans rigueur*, LGDJ, Anthologie du droit, 2013.

différents pays, l'évolution du droit PNR doit prendre en compte les accords internationaux conclus en matière de transferts de données transfrontaliers, comme le RGPD ou des accords bilatéraux, en vue de garantir que ces transferts soient effectués conformément aux exigences normatives.

La protection juridique des dossiers passagers se trouve alors confrontée à différents types d'obstacles et la problématique principale qui se pose est de savoir de quelle manière la protection juridique des dossiers passagers se heurte à des limites dont la nature varie selon le temps.

Dans une première partie, les limites traditionnelles à la protection juridique des dossiers passagers seront étudiées, en relevant que celles-ci résultent de la prééminence d'actes juridiques et de législations à visée répressive qui viennent empiéter sur les droits fondamentaux des passagers aériens, notamment le droit à la protection des données à caractère personnel des passagers aériens. Dans une seconde partie, les nouvelles menaces qui pèsent sur la protection juridique des dossiers passagers seront examinées, en soulignant que celles-ci ont pour racine l'altération des frontières dans le contexte contemporain et le phénomène de déterritorialisation qui n'épargne pas l'espace où sont traités et transférés les dossiers passagers. Bien que l'objectif de cette étude ne soit pas de procéder à une analyse détaillée des cadres juridiques national, européen et international des dossiers passagers compte tenu du caractère mondial des données personnelles des passagers aériens, les spécificités européennes, françaises et américaines seront particulièrement étudiées, suivant une perspective de droit comparé, afin d'explicitier certains aspects juridiques et leurs conséquences.

PARTIE I – LES LIMITES TRADITIONNELLES À LA PROTECTION JURIDIQUE DES DOSSIERS PASSAGERS

La recherche d'un équilibre entre la sécurité collective et la protection des droits fondamentaux est un défi permanent pour les gouvernants⁶⁹. En effet, assurer la sécurité de la collectivité sans porter atteinte aux libertés des citoyens est l'une des missions que doit remplir l'État⁷⁰. Or, s'agissant des données personnelles des dossiers passagers aériens, cet équilibre est mis à mal par la prééminence des législations répressives qui limitent leur protection juridique (Titre 1). Néanmoins, un arsenal normatif est mis en place par le législateur européen et les États membres afin de protéger la masse de données des passagers aériens que l'activité des transporteurs aériens produit. Du règlement (UE) n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données au droit national (RGPD)⁷¹, en passant par la directive 2016/681 du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers (PNR)⁷² pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, les règles s'accumulent pour encadrer l'utilisation et la transmission des données personnelles des passagers aériens.

⁶⁹ S. MANACORDA, « Le droit pénal sous Lisbonne : vers un meilleur équilibre entre liberté, sécurité et justice », *Revue de Science criminelle et de droit pénal comparé*, 2010. L'auteur cite le souhait du Conseil dans le cadre du Traité de Lisbonne de « garantir le respect des libertés fondamentales et l'intégrité de la personne, tout en assurant la sécurité en Europe. Il est primordial que les mesures répressives et les mesures permettant de préserver les droits de la personne, l'État de droit et les règles relatives à la protection internationale aillent dans le même sens et soient complémentaires ». Voir également, S. MANACORDA, « Reconnaissance mutuelle et droits fondamentaux dans l'espace de liberté, de sécurité et de justice de l'Union européenne : un développement inégal », *Revue de Science criminelle et de droit pénal comparé*, 2006, pp. 881 s.

⁷⁰ T. HOBBS, *Léviathan*, 1651. Dans son essai de référence, Hobbes développe sa théorie du contrat social et affirme que les individus acceptent de renoncer à une partie de leur liberté en échange de la protection de l'État, qui doit garantir la sécurité et la stabilité de la société. Aussi, John Locke a abordé la mission de l'État pour assurer la sécurité des citoyens dans son œuvre *Deux traités du gouvernement civil* (Two Treatises of Government) publié en 1689. Locke soutient que l'État a pour mission de protéger les droits naturels des individus, notamment le droit à la vie, à la liberté et à la propriété. Si l'État ne remplit pas cette mission, les citoyens sont alors susceptibles de se révolter.

⁷¹ Le règlement (UE) n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données au droit national (RGPD) a été longuement commenté dans la doctrine du fait de son caractère à la fois protecteur et innovateur. V. La mise en conformité par la CNIL au Règlement général sur la protection des données (RGPD) : premier bilan un an après Thomas Dautieu, Propos recueillis par Béa Arruabarrena dans I2D – Information, données & documents 2019/1 (n° 1), pages 25 à 28 en ligne à URL : <https://www.cairn.info/revue-i2d-information-donnees-et-documents-2019-1-page-25.htm> consulté le 18 septembre 2023.

⁷² 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. V. S. PEYROU-BARTOLL, « Nouvelles technologies, sécurité et protection des données à caractère personnel : un cadre juridique européen à la hauteur des enjeux ? », *Cahiers de la sécurité et de la justice*, 2022, pp.186-196.

Permettant l'identification de personnes physiques, les données des dossiers passagers sont aujourd'hui collectées et utilisées par les transporteurs à tous les stades de la réalisation de leurs opérations : de la réservation des vols au débarquement des voyageurs. Leur utilisation est particulièrement sensible car leur communication à des personnes ou entités non autorisées pourrait en effet être susceptible de porter atteinte aux droits et libertés des personnes faisant l'objet d'une collecte de leurs données⁷³. Bien qu'au départ pensé comme un système à visée commerciale, le système PNR actuel complète les outils existants pour lutter contre la criminalité transfrontière et les infractions terroristes. Le traitement des données PNR permet aux autorités répressives d'identifier des individus qui ne sont pas initialement suspects d'activités criminelles ou terroristes, mais dont une analyse ultérieure des données suggère qu'ils pourraient l'être. La France, les États-Unis, la Grande-Bretagne et d'autres États se sont dotés d'un système PNR national⁷⁴.

Les données des passagers aériens se sont effectivement révélées être un outil de renseignement efficace puisqu'elles ont permis de briser des réseaux de grande criminalité⁷⁵. De manière générale, compte tenu des développements de la coopération internationale dans les aéroports, la prévention contre les infractions terroristes est à l'origine d'une considérable augmentation des traitements automatisés de données à caractère personnel⁷⁶.

Dans ce contexte, le Conseil de sécurité des Nations unies encourage une politique de lutte contre le terrorisme à travers notamment le vote de résolutions appelant les États membres à adopter un arsenal juridique conséquent. Dans le cadre de cette lutte, a été votée le 21 décembre 2017 la résolution 2396 dans laquelle les États membres étaient appelés à collecter les données des passagers aériens pour empêcher le retour des combattants terroristes étrangers. Le Conseil de sécurité a en effet explicitement « exhort[é] les États membres à envisager, le cas échéant, de déclasser, à des fins administratives, les données de renseignement, y compris les données relatives aux voyages (...), afin de les communiquer (...) et de les transmettre comme il convient aux autres États et organisations internationales compétentes concernés (...) »⁷⁷. L'utilisation des données des dossiers passagers permet de

⁷³ P. SIMON, « L'action de groupe et le RGPD en matière de transport aérien », *Activités touristiques - Données personnelles*.

⁷⁴ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, 2016/2, p. 111.

⁷⁵ S. SUTOUR et Y. DETRAIGNE, « Rapport N°401 : La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives », Commission des lois, *Sénat*, 13 mai 2009, en ligne à URL : <http://www.senat.fr/ue/pac/E6014.html> consulté en ligne le 23 mars 2023.

⁷⁶ Y. MAYAUD, « Répertoire de droit pénal et de procédure pénale », *Terrorisme – Prévention*, *Dalloz*, janvier 2018.

⁷⁷ Conseil de sécurité, Résolution 2396 (2017), ONU.

tracer les déplacements des personnes dans le but de prévenir la commission d'actes terroristes. Le recours à cette base de données est devenue une pratique courante. L'intégration de l'informatique dans les systèmes aéroportuaires offre des possibilités presque infinies d'analyse et de croisement de ces données à caractère personnel des passagers⁷⁸.

Cela n'a pas empêché des critiques qui se sont élevées pour souligner les dangers que peut constituer l'utilisation de ces données si le législateur n'encadre pas la durée de leur conservation et l'instance indépendante chargée de les traiter. Le risque pourrait être, par exemple, une utilisation de données sensibles portant des opinions religieuses ou politiques. Ces questions ont été soulevées aussi bien sur le plan national, par les parlementaires français notamment, qu'au niveau de l'Union européenne, par les députés européens⁷⁹, et international. La sûreté aérienne, qui inclut notamment la lutte contre le terrorisme, est un défi global et les débats autour des fichiers PNR cristallisent une tension continue entre sûreté et liberté.

L'empiètement de ces législations répressives sur les droits fondamentaux des passagers aériens (Titre 2) est une autre limitation à une protection effective des dossiers passagers. Un avis des juges de Luxembourg rendu le 26 juillet 2017⁸⁰ a relancé les débats sur la compatibilité du système PNR avec la protection des données personnelles et des libertés fondamentales en général. La Cour de justice de l'Union européenne (CJUE) était en l'espèce appelée à se prononcer sur un projet d'accord entre le Canada et l'Union européenne relatif à un transfert de données de passagers aériens. En constatant l'incompatibilité de l'accord en question avec les droits fondamentaux garantis par les traités européens, les juges ont souhaité assurer un très haut niveau de protection des données personnelles des passagers aériens, considérant que les droits fondamentaux des citoyens européens ne devaient pas être sacrifiés sur l'autel des impératifs sécuritaires⁸¹. Dans un contexte international marqué par des actes terroristes défrayant la chronique, le droit à la protection des données à caractère personnel n'apparaît pas comme un droit absolu. Il semble ainsi être considéré par rapport à sa fonction dans la société et est mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité notamment rappelé dans l'avis 1/15 sur l'accord PNR UE-Canada précité rendu par la CJUE⁸². L'équilibre entre le droit au respect de la vie privée et à la

⁷⁸ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.

⁷⁹ C. BILLET, « L'échange et la protection de données avec les États tiers : un nouveau volet prioritaire de l'action extérieure de l'Union ? », *Revue trimestrielle de droit européen*, 2020.

⁸⁰ CJUE, Avis 1/15 de la Cour (grand chambre), 26 juillet 2017.

⁸¹ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *Communication – Commerce électronique*, n° 6, LexisNexis, juin 2018.

⁸² Ibidem

protection des données à caractère personnel, d'un côté, et la sécurité collective, de l'autre, est toutefois susceptible de varier à travers le monde.

La répression pénale, à travers la législation, apparaît comme le reflet d'une volonté de protéger les valeurs fondamentales que revendique une société, en condamnant ainsi un comportement qu'elle réprouve⁸³. Par conséquent, l'infraction pénale est porteuse d'un « message moral beaucoup plus fort qu'une sanction civile ou administrative »⁸⁴. La sanction pénale est notoirement privative de liberté. Cette exigence normative, à travers le risque de sanction pénale, se veut dissuasive, invitant les individus à se plier aux lois de la société⁸⁵. Dans le cas des législations qui luttent contre le terrorisme, dont le régime pénal se veut d'exception, le caractère répressif est, *a fortiori*, plus nettement caractérisé. C'est dans ce contexte, par exemple, que la loi du 30 octobre 2017⁸⁶ a renforcé la sécurité intérieure et la lutte contre le terrorisme, en pérennisant le régime permettant la consultation des données du fichier des passagers du transport aérien. Demeure néanmoins la crainte que la logique répressive soit détournée de son objectif initial, celui de lutter contre les infractions terroristes, pour réprimer l'action politique. Il s'agit de la critique émise par Raphaël Kempf⁸⁷ dans son ouvrage intitulé *Ennemis d'État*. À ce titre, le juriste constate : « des milliers de gens [qui] sont placés en garde à vue et qu'une faible partie est effectivement condamnée, on peut en déduire que la garde à vue ne sert plus à caractériser les éléments d'une infraction pénale mais à maintenir l'ordre en écartant des gens de la manifestation »⁸⁸.

⁸³ C. BECCARIA, *Des délits et des peines*, 1764. Dans cet ouvrage, qui figure parmi les œuvres fondatrices de la criminologie moderne, Beccaria considère que la répression pénale est conçue pour protéger les citoyens et la société au lieu de venger. L'auteur italien soutient également que les peines doivent être proportionnées aux délits commis et le système pénal doit être basé sur des principes de prévisibilité, de dissuasion et de justice.

⁸⁴ L. BERNARDEAU, « Section 2. – La responsabilité pénale, *Les amendes en droit de la concurrence*, Bruxelles », Larcier, 2013, p. 961.

⁸⁵ E. DURKHEIM, *La division du travail social*, 1893. Durkheim soutient que la sanction pénale moderne est cruciale dans le maintien de la cohésion sociale en réaffirmant les valeurs et normes communes, reflétant ainsi la solidarité collective de la société.

⁸⁶ Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme. V. J. ALIX, O. CAHN, « Mutations de l'antiterrorisme et émergence d'un droit répressif de la sécurité nationale », *Revue de science criminelle et de droit pénal comparé*, 2017, pp. 845-868.

⁸⁷ R. KEMPF, *Ennemis d'États. Les lois scélérates des anarchistes aux terroristes*, La Fabrique éditions, 2019.

⁸⁸ N. SWEENEY, « Raphaël Kempf : 'Il y a une criminalisation de l'action politique' », *Politis*, 11 janvier 2023, en ligne à URL : <https://www.politis.fr/articles/2023/01/il-y-a-une-criminalisation-de-laction-politique-raphael-kempf/> consulté en ligne le 18 février 2022.

TITRE 1 – LA PRÉÉMINENCE DES LÉGISLATIONS RÉPRESSIVES EN MATIÈRE DE DOSSIERS PASSAGERS

Le sujet de la protection des données personnelles des passagers aériens a été dominé, au début du XX^e siècle, par un antagonisme entre les législations répressives américaine et européenne relatives à la transmission des dossiers passagers (chapitre 1). Traditionnellement, le droit répressif est défini, comme le rappelle Marie-Anne Cohendet, comme « le droit qui sanctionne les personnes qui ne sont pas soumises à la règle préétablie »⁸⁹. En effet, dès lors que les règles sociales ne sont pas toujours respectées, il est nécessaire de prévoir la répression des atteintes à ces règles⁹⁰.

Pour la doctrine, ce n'est pas seulement le droit pénal mais plus largement l'ensemble des dispositifs répressifs qui punissent en prévoyant une sanction⁹¹. Cette vocation répressive s'est consolidée après les attentats du 11 septembre 2001 puisque cet événement tragique a incité les États à renforcer leur contrôle sur les données des passagers aériens. Dans ce cadre, les données PNR ont été employées à deux fins principales : premièrement, pour évaluer le risque présenté par les passagers avant leur arrivée ou leur départ, en se basant sur des critères de risque préétablis ; deuxièmement, pour identifier des individus spécifiques afin de développer ces critères de risque et dans le cadre d'enquêtes ou de poursuites ciblées.

Cet empiètement sur les droits fondamentaux reposerait sur un objectif légitime tel qu'il a été reconnu par la CJUE dans l'avis 1/15 précité. En effet, selon les juges européens, le traitement des données des passagers répond à une finalité d'intérêt général, la protection de la sécurité publique « susceptible de justifier des ingérences, même graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte »⁹². Cette position a voulu dissiper les inquiétudes de celles et ceux qui doutent de la compatibilité du système PNR avec le droit de l'Union européenne.

⁸⁹ M.-A. COHENDET, « Le droit répressif, quelles valeurs, quelles frontières ? », *Revue juridique de l'environnement*, Lavoisier, 2014.

⁹⁰ M. FOUCAULT, *Surveiller et punir*, Gallimard, 1975. Le philosophe français Foucault analyse l'évolution des systèmes de punition et de contrôle social en Europe, en mettant l'accent sur le passage de méthodes punitives violentes et publiques à des formes de surveillance et de répression plus institutionnalisées et subtiles. L'auteur examine également comment le système pénal a évolué pour devenir un outil de contrôle social plus discret, impliquant des institutions telle que la prison.

⁹¹ T. BINGHAM, *The rule of law*, Allen Lane, 2020. Le juriste britannique Tom Bingham souligne dans cet essai la nécessité pour l'État de garantir la liberté individuelle et la protection des droits fondamentaux des citoyens. Aussi, il considère que le droit répressif doit être exercé de façon équilibrée afin de préserver les droits individuels des citoyens et les valeurs fondamentales d'une société moderne. V. R. MORGAN, *The Rule of Law*. By Tom Bingham, *The British Journal of Criminology*, Volume 50, Issue 6, November 2010, Pages 1202–1205.

⁹² CJUE, Avis 1/15 de la Cour (grand chambre), 26 juillet 2017, pt. 149.

Les accords signés entre l'UE et d'autres États visant à permettre aux transporteurs de l'UE de transférer des données PNR aux États-Unis, à l'Australie et au Canada⁹³ reposent sur l'idée que le droit à la vie privée et le droit à la protection des données personnelles peuvent recevoir des limitations dès lors que la collecte des données des dossiers passagers vise à permettre une réponse proactive face à des attaques par nature difficilement saisissables. Un consensus des législations répressives sur la finalité sécuritaire des dossiers passagers justifiant une limitation des libertés a vu le jour (chapitre 2). En effet, dans un État de droit, le régime répressif se présente comme un aménagement des libertés publiques puisque les juristes considèrent que « la liberté s'exerce souverainement dans un cadre de limites qu'elle ne transgressera pas sans sanction pénale »⁹⁴, cadre que le législateur va définir.

En l'occurrence, l'utilisation des données des passagers aériens s'insère dans la stratégie européenne de lutte contre le terrorisme. Adoptée en 2005 par le Conseil, celle-ci vise à combattre « le terrorisme à l'échelle mondiale et rendre l'Europe plus sûre »⁹⁵ pour les individus présents dans cet espace. Cette stratégie européenne repose sur quatre piliers : la prévention, la protection, la poursuite et la réaction. Comme deuxième priorité de la stratégie européenne, la protection comprend la protection des frontières extérieures, la protection des cibles stratégiques, le renforcement de la sécurité dans les transports et la réduction de la vulnérabilité des infrastructures critiques. La volonté de protéger les citoyens et les infrastructures ainsi que de réduire leur vulnérabilité aux attentats a alors poussé l'Union européenne à adopter en avril 2016 la directive PNR⁹⁶.

Pour Jean-Paul Jacqué, la politique européenne des dossiers passagers fait partie des sujets « non-négligeables » au sein de l'espace de l'Union européenne depuis plusieurs années, cela bien qu'elle n'ait pas été mise en avant lors des débats politiques des dernières élections européennes⁹⁷.

⁹³ P. BERTHELET, « Tous les chemins mènent... à Luxembourg. Analyse institutionnelle de l'accord PNR UE-Canada », *RDLF*, Droit de l'Union européenne, Chronique n° 20, 2018 en ligne à URL : <https://revuedlf.com/droit-ue/tous-les-chemins-menent-a-luxembourg-analyse-institutionnelle-de-laccord-pnr-ue-canada/> consulté le 18 septembre 2023.

⁹⁴ B. PELLEGRINI, « Logique préventive et droit des libertés publiques », *La revue lacanienne*, 2007, pp. 82-85.

⁹⁵ Conseil de l'Union européenne, *Stratégie européenne de sécurité – Une Europe sûre dans un monde meilleur*, 2009, p.43, en ligne à URL : <https://www.consilium.europa.eu/media/30810/qc7809568frc.pdf> consulté le 18 septembre 2023.

⁹⁶ 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.

⁹⁷ J.-P. JACQUÉ, « Une élection de 'second ordre' ? », *Revue trimestrielle de droit européen*, 2019.

Les négociations portant sur les données PNR se sont souvent déroulées dans des conditions ardues dans lesquelles le Parlement européen a très tôt regretté « l'absence de tout contrôle démocratique, le nouvel accord PNR, qui résulte des exigences américaines, ayant été négocié et conclu sans la moindre participation du Parlement européen et en ne laissant aux parlements nationaux que des possibilités insuffisantes d'influer d'une quelconque manière sur le mandat de négociation, ni d'évaluer de façon approfondie le nouvel accord PNR proposé ou de présenter des amendements »⁹⁸. Cette préoccupation sur l'insécurité juridique a créé et nourri les critiques du Parlement européen sur le niveau insuffisant de protection des données passagers aériens. En effet, ce dernier déplorait « l'absence de dispositions claires et proportionnées sur le partage de l'information, la conservation des données et le contrôle par les autorités de protection des données »⁹⁹. En conséquence, le Parlement européen a exprimé des réserves concernant l'accord PNR en 2007 et a cherché à renégocier certaines de ses dispositions pour mieux protéger les droits fondamentaux des citoyens européens. Des négociations ultérieures ont abouti à un nouvel accord PNR en 2012, qui comportait certaines améliorations en matière de protection des données et de droits des passagers, bien que des inquiétudes concernant le droit à la vie privée et le droit à la protection des données à caractère personnel continuent d'exister¹⁰⁰.

⁹⁸ Parlement européen, *Résolution du Parlement européen du 12 juillet 2007 sur l'accord avec les États-Unis d'Amérique concernant l'utilisation de données des dossiers des passagers aériens (PNR)*, 12 juillet 2007.

⁹⁹ Ibidem

¹⁰⁰ C. VALLET, « Fichés jusqu'au ciel ? », *Alternatives économiques*, 2015, p. 19. V. D. BIGO, L. BONELLI, T. DELTOMBE, « Les libertés sacrifiées au nom de la sécurité ? » in *Au nom du 11 septembre... Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, 2008, Introduction. V. F. DUBUISSON, « La définition du 'terrorisme' : débats, enjeux et fonctions dans le discours juridique », *Confluences méditerranée*, 2007, pp. 29-45. Le débat autour du PNR renvoie nécessairement à la politique antiterroriste des pays concernés.

Chapitre 1 – L’antagonisme entre les législations répressives relatives à la transmission des dossiers passagers

Victor Hugo écrivait « Après tout, l'antagonisme fait saillir l'être »¹⁰¹, une idée qui trouve écho dans la manière dont les législations répressives sur la transmission des données passagers ont émergé sur la scène juridique, comme une force émergeant devant le monde. Le développement de l'utilisation des données personnelles des utilisateurs du transport aérien n'a été possible qu'avec l'essor du transport aérien de masse et celui des nouvelles technologies. Ces dernières peuvent remettre en question les cadres juridiques existants, créer de nouveaux défis et opportunités, et avoir un impact profond sur la société et l'économie. Plus précisément, elles entraînent des conséquences significatives sur les sujets liés à la vie privée, à la cybersécurité et la protection des données à caractère personnel¹⁰².

Dans le même temps, le développement des activités criminelles n'a pas été moins rapide. Depuis les années 1970, les États européens, dont la France, ont été confrontés à plusieurs vagues d'actes terroristes¹⁰³. Des lois antiterroristes ont été adoptées, à chaque fois, pour prévenir de nouveaux attentats¹⁰⁴. Dans les années 1980, le législateur a estimé que les affaires terroristes ne devaient plus être du domaine des juridictions ordinaires. À titre d'exemple, le 9 septembre 1986¹⁰⁵, la France a voté la loi relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État qui définit la notion de terrorisme et en tire des conséquences procédurales, dont l'incrimination de l'apologie de terrorisme, l'extension de la durée de la garde à vue à quatre jours, le report de l'intervention de l'avocat à la 72^e heure de garde à vue, l'alourdissement des peines, l'indemnisation des victimes de terrorisme alimentée par un fonds prélevé sur les assurances privées, l'autorisation des perquisitions domiciliaires même sans l'assentiment des personnes suspectées, l'exemption de peines pour

¹⁰¹ V. HUGO, *Océan Prose*, in *Œuvres complètes*, 1854, R. Laffont, 1995.

¹⁰² M. BOUGEOIS, L. THIBIERGE, « Droit de la donnée : plaidoyer pour un régime général », Données personnelles, *La Semaine Juridique Entreprise et Affaires*, n° 20, 14 mai 2020. Les deux auteurs plaident pour l'édiction d'un « droit commun » de la donnée au vu du rôle central que joue aujourd'hui la donnée dans les sociétés contemporaines, notamment dans le domaine de l'intelligence artificielle.

¹⁰³ G. FERRAGU, « En rouge et noir, une génération en guerre civile », in *Histoire du terrorisme*, Perrin, 2014, pp. 376-428.

¹⁰⁴ J-E. GICQUEL, « Le droit de l'antiterrorisme - Un droit aux confins du droit administratif et du droit pénal », *La Semaine juridique Édition générale*, n° 40, 2 octobre 2017. Ensemble, le droit administratif et le droit pénal constituent, d'après l'auteur, le droit de l'antiterrorisme qui pose des limitations croissantes à l'exercice des libertés fondamentales en France.

¹⁰⁵ Loi n° 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme. Cette loi a été promulguée en réponse à une série d'actes terroristes qui avaient eu lieu en France à cette époque, principalement perpétrés par des groupes basques séparatistes, comme l'ETA, et des militants nationalistes corses.

des criminels qui empêchent la réalisation d'un attentat. Ce texte a aussi créé un corps spécialisé de juges d'instruction et de procureurs, composant le service central de lutte antiterroriste, communément appelé la 14^e section du parquet, pour traiter tous les dossiers de terrorisme. De plus, pour juger les crimes terroristes, ont été institués des procès devant des magistrats professionnels à la Cour d'assises de Paris, faisant ainsi exception à la règle du procès de Cour d'assises devant un jury populaire. Durant les années 1990 et jusqu'en 2004, d'autres lois viendront renforcer cette dynamique¹⁰⁶.

Après 2006, les lois de lutte contre le terrorisme ont commencé à prendre en compte les enjeux de cyberterrorisme. Ainsi, la loi du 23 janvier 2006¹⁰⁷, à travers son article 6, a imposé aux opérateurs télécoms, aux fournisseurs d'accès Internet (FAI) et à tout établissement public proposant un accès au net, comme les commerces louant une connexion à internet, de conserver les données de connexion (logs) pendant un an. Cette loi permet que l'accès à ces logs, par les autorités policières, ne soit plus soumis à l'autorisation d'un magistrat, et donc effectué sous contrôle judiciaire. Dorénavant, l'accès est simplement soumis à celle d'un haut fonctionnaire de la police nommé par la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Saisi sur la question du passage d'un contrôle judiciaire à un contrôle administratif, le Conseil constitutionnel a considéré que la lutte contre le terrorisme n'était pas exclusivement du domaine judiciaire¹⁰⁸.

Le 13 novembre 2015, des attentats terroristes ont été perpétrés à Paris et à Saint-Denis en faisant plusieurs centaines de victimes¹⁰⁹. Le jour suivant, le Conseil des ministres a adopté un

¹⁰⁶ J.-C. PAYE, « Lutte antiterroriste et contrôle de la vie privée », *Multitudes*, 2003, pp. 91-105, en ligne à URL : <https://www.caim.info/revue-multitudes-2003-1-page-91.htm> consulté le 19 septembre 2023.

¹⁰⁷ Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers. V. le rapport déposé par le député français Alain Marsaud le 16 novembre 2005 où l'auteur considère que les démocraties doivent éviter deux écueils : « angélisme » et remise en cause de « l'État de droit » - rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi (n° 2615), après déclaration d'urgence, relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

¹⁰⁸ Conseil constitutionnel, décision n°2005-532 DC du 19 janvier 2006, sur la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers. Lire en sens. J.-C. KROSS, « État des lieux de la lutte contre le terrorisme en France », *Revue française de criminologie et de droit pénal*, n° 8, avril 2017. Voir également. S. LAURENT, *Politiques du renseignement*, Pessac, Presses universitaires de Bordeaux, 2009. V. L'audition devant le Sénat de M. Jean-Marie DELARUE, le 16 décembre 2015, comme président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS). Ce dernier rappelle les finalités des interceptions : la prévention de la criminalité et de la délinquance organisées ; la prévention du terrorisme ; les atteintes à la sécurité, espionnage et contre-espionnage ; les atteintes aux activités économiques essentielles de la Nation ; les actions de reconstitution de groupements de fait ou de droit dissous par le Gouvernement, en ligne à URL : https://www.senat.fr/compte-rendu-commissions/20150914/ce_aai.html#toc4 consulté le 20 septembre 2023.

¹⁰⁹ G. SALINES, *L'Indicible de A à Z*, Seuil, Paris, 1er septembre 2016. V. Le Figaro, « Attentats de Paris : le point sur l'enquête 24 heures après les faits », 13 novembre 2015, en ligne à URL : <https://www.lefigaro.fr/actualite-france/2015/11/14/01016-20151114ARTFIG00228-attentats-de-paris-le-point-sur-l-enquete-24-heures-apres-les-faits.php> consulté le 19 septembre 2023.

décret déclarant l'état d'urgence pour une durée de 12 jours. En Île-de-France, un décret spécifique a été publié. Ces décrets ont accordé le droit aux préfets de restreindre les déplacements, de fermer des lieux de réunion, d'interdire le séjour dans certaines parties du territoire à toute personne susceptible de créer un trouble à l'ordre public ainsi que d'assigner à résidence des individus dont l'activité s'avère dangereuse pour la sécurité et l'ordre public. Le 15 novembre, un décret est publié déclarant trois jours de deuil national en hommage aux victimes des attentats du 13 novembre¹¹⁰. Le jour d'après, le 16 novembre 2015, le Président de la République, en application de l'article 18 de la Constitution, a convoqué le Congrès, réunissant les députés et les sénateurs, pour faire une déclaration qui annonça les décisions suivantes : intensification des opérations françaises en Syrie, présentation d'un projet de loi prolongeant l'état d'urgence, demande d'une réunion du Conseil de sécurité de l'ONU dans les meilleurs délais pour adopter une résolution de lutte contre le terrorisme, révision de la Constitution pour « agir contre le terrorisme de guerre », création de postes supplémentaires dans les forces de sécurité notamment parmi la police, la gendarmerie, les douanes et la justice. Plusieurs autres projets ont été annoncés et certains ont été abandonnés comme le projet de loi constitutionnelle « de protection de la Nation », qui prévoyait, outre la constitutionnalisation de l'état d'urgence, la déchéance¹¹¹ de la nationalité pour un crime ou un délit constituant une atteinte grave à la vie de la nation¹¹².

En 2021, deux lois ont été votées renforçant l'arsenal anti-terroriste français. D'une part, le 30 juillet 2021, une loi relative à la prévention d'actes de terrorisme et au renseignement a été prise¹¹³. Ce texte visait plusieurs objectifs. D'abord, il a pérennisé et adapté certaines mesures de lutte contre le terrorisme expérimentées depuis la loi renforçant la sécurité intérieure et lutte contre le terrorisme, dite « loi SILT », du 30 octobre 2017¹¹⁴. Cette législation prévoyait l'extension jusqu'à deux ans cumulés - au lieu d'un an - des mesures administratives de

¹¹⁰ A. WAGENER, « Réactions post-attentats en France et en Belgique : étude comparative des discours de l'exécutif politique », *Mots. Les langages du politique*, n° 116, 2018, pp.111-130. Voir. S. AUDOIN-ROUZEAU, « L'après-13 Novembre, Naissance et mort d'une 'culture de guerre' ? », *Vingtième siècle. Revue d'histoire*, n° 134, 2017, p. 11. Voir également V. BRENGARTH, « Le procès des attentats du 13 novembre est symptomatique des déficiences de la justice antiterroriste », *Le Monde*, 25 juillet 2022.

¹¹¹ J.-L. RONGÉ, « Déchéance : à propos du projet de révision constitutionnelle concernant les binationaux condamnés pour terrorisme - Du sentiment renforcé d'être différent », *Journal du droit des jeunes*, n°350, 2015, pp. 9-17.

¹¹² Le Conseil d'État dans son avis (n° 390866) du 11 décembre 2015 sur le projet de loi constitutionnelle a convaincu les rédacteurs du projet à étendre le champ d'incriminations. Il considère « qu'il ne serait pas opportun d'introduire le terme « terrorisme » dans la Constitution et qu'il est par conséquent préférable de prévoir que la déchéance pourrait être infligée exclusivement aux personnes « condamnées pour un crime constituant une atteinte grave à la vie de la Nation ». Il appartenait au législateur de préciser quelles sont les infractions qui entrent dans ce champ, étant entendu qu'il ne peut s'agir que de crimes en matière de terrorisme et, éventuellement, des crimes les plus graves en matière d'atteinte aux intérêts fondamentaux de la Nation ».

¹¹³ Loi n°2021-988 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

¹¹⁴ Loi n°2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

surveillance (MICAS) pour les personnes sortant de prison et condamnées à une lourde peine de prison pour terrorisme. Cette dernière proposition a été censurée par le Conseil constitutionnel du fait de la rigueur des interdictions et des obligations pouvant être prononcées à l'occasion d'une telle mesure¹¹⁵. De plus, le texte a créé une nouvelle « mesure judiciaire de prévention de la récidive terroriste et de réinsertion » destinée aux personnes particulièrement dangereuses¹¹⁶. Cette disposition remplace les mesures de sûreté voulues par la loi du 10 août 2020, dite « loi Braun-Pivet », que le Conseil constitutionnel avait censurée. Enfin, cette loi a renforcé la législation sur le renseignement de 2015 qui avait mis en place un recours accru aux algorithmes et une possibilité, à titre expérimental, d'intercepter des communications satellitaires. D'autre part, le 24 août 2021, la France a voté la loi confortant le respect des principes de la République¹¹⁷ en réponse à l'assassinat terroriste de l'enseignant Samuel Paty¹¹⁸, tué en octobre 2020. Elle établit notamment un délit d'entrave à la fonction d'enseignant¹¹⁹.

En France, les actes de terrorisme figurent dans le Code pénal parmi les crimes et délits contre la Nation, l'État et la paix publique¹²⁰. Les actes terroristes ont en commun d'être commis intentionnellement et en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par la terreur ou l'intimidation¹²¹. En ce sens, les textes qui promeuvent les systèmes PNR peuvent être définis comme des législations répressives qui visent à sanctionner les infractions à caractère terroriste et les crimes transnationaux.

Le transport aérien, comme toute autre activité humaine, n'est pas à l'abri de crimes commis dans d'autres domaines. Il a été en effet au centre de l'un des événements les plus tragiques de ce début de siècle : les attentats terroristes du 11 septembre 2001. Ce jour funèbre a eu un impact retentissant, aussi bien sur la politique intérieure américaine, que dans la relation des États-Unis avec les autres États. Sur le plan juridique, ces derniers ont unilatéralement imposé

¹¹⁵ Conseil constitutionnel, décision n°2021-822 DC du 30 juillet 2021.

¹¹⁶ Loi n° 2021-988 relative à la prévention d'actes de terrorisme et au renseignement, 30 juillet 2021, Article 6.

¹¹⁷ Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République, 25 août 2021.

¹¹⁸ C. MESTRE, S. MINASSIAN, M. R. MORO, « Ondes de choc après l'assassinat de Samuel Paty », *L'autre*, 2021, pp. 4-6, en ligne à URL : <https://www.cairn.info/revue-l-autre-2021-1-page-4.htm> consulté le 20 septembre 2023. Voir F. TRUONG, « Le drame de Conflans-Sainte-Honorine nous rappelle qu'une salle de classe n'est pas une arène politique publique », *Le Monde*, 2020, en ligne à URL : http://www.lemonde.fr/idees/article/2020/11/23/fabien-truong-le-drame-de-conflans-sainte-honorine-nous-rappelle-qu-une-salle-de-classe-n-est-pas-une-arene-politique-publique_6060745_3232.html consulté le 20 septembre 2023.

¹¹⁹ Loi n°2021-1109 du 24 août 2021, Article 10. Code pénal, article 431-1. Lire en sens. P. JANUEL, « Séparatisme : les principales dispositions de la loi », *Dalloz*, Administratif – Pénal, 7 septembre 2021, en ligne à URL : <https://www.dalloz-actualite.fr/flash/separatisme-principales-dispositions-de-loi> consulté le 20 septembre 2023.

¹²⁰ Code pénal, Livre IV : Des crimes et délits contre la nation, l'État et la paix publique, Articles 410-1 à 450-5.

¹²¹ Terrorisme (définition) in Fiche d'orientation, *Dalloz*, 2021.

aux avions entrants, sortants ou en transit sur leur sol national, de transmettre les données personnelles de passagers aériens¹²². Cette obligation a ouvert un nouveau chapitre dans le domaine du droit aérien américain mais également en matière de droit international. Elle a eu des implications certaines sur les droits fondamentaux et les libertés publiques (Section 1), en mettant les États et les compagnies aériennes devant le fait accompli. L'Union européenne a été la première à réagir en contestant cette nouvelle obligation de transmission à travers l'activité législative de ses institutions. Ces dernières ont mis en avant une logique juridique d'équilibre entre le respect des droits individuels et l'instauration d'un impératif de sécurité collective (Section 2)¹²³.

Du PNR à la réforme du Code Schengen, en passant par la création d'un corps de garde-frontières européens renforcé, le législateur de l'Union a voulu envoyer un message rassurant aux citoyens européens pour montrer que leurs préoccupations relatives à l'immigration et au terrorisme n'étaient pas restées lettre morte¹²⁴. Il existe toutefois une défiance dans la communauté des juristes européens vis-à-vis des dispositifs PNR qui n'a pas disparu. Ainsi, pour le Contrôleur européen de la protection des données (CEPD), « le PNR a peu d'utilité pratique, coûte très cher et ses délais très longs de mise en œuvre ne répondent pas aux besoins des forces de l'ordre dans une phase d'urgence »¹²⁵. Ainsi, le CEPD a pu conclure dans son avis sur l'accord UE-Canada qu'« à cette date, [il] n'est pas convaincu par les éléments démontrant la nécessité et la proportionnalité du traitement massif et quotidien des données concernant les passagers qui ne sont pas considérés par les services de police comme suspects »¹²⁶.

¹²² La collecte des données PNR auprès des transporteurs aériens est prévue par la législation américaine 49 U.S.C. § 44909(c)(3) et ses règlements d'application à 19 C.F.R. § 122.49d.

¹²³ A. GARAPON, « Les dispositifs antiterroristes de la France et des États-Unis », *Esprit*, n° 327, août-septembre 2006, pp. 125-149. L'auteur considère que la stricte et exclusive opposition entre libertés et sécurité est une approche répandue et réductrice, car on ne peut juger un appareil sécuritaire exclusivement au regard des atteintes qu'il cause aux droits individuels. La rationalité interne du système sécuritaire peut être aussi jugé selon ses méthodes et sa finalité.

¹²⁴ J. JEANDESBOZ, « Ceci n'est pas un contrôle : PNR Data Processing and the Reshaping of Borderless Travel in the Schengen Area », *European Journal of Migration and Law*, 2021, pp. 431-456.

¹²⁵ Coullisses de Bruxelles, « PNR: un fichier des voyageurs aériens inutile », 21 décembre 2015.

¹²⁶ CEPD, 30 septembre 2013, considérant 3, en ligne à URL : https://edps.europa.eu/system/files/2021-04/20-11-20_formal_comments_mutual_recognition_eu-canada_customs_final_fr.pdf consulté le 18 novembre 2023.

Section 1 – L’obligation de transmission imposée par le droit américain

« Washington ! le gouvernement fédéral, le législateur abstrait, l’ogre centralisateur, la menace potentielle pour les libertés locales... Aux États-Unis, il n’y a jamais eu, sauf montée en puissance depuis la seconde mondiale, de pouvoir central fort ». Ces propos introductifs de Jean Cedras à son ouvrage sur le droit pénal américain évoquent sans détours la crainte historique des citoyens américains vis-à-vis d’un pouvoir fédéral puissant et surplombant les États fédérés en leur imposant telle ou telle législation¹²⁷. Historiquement, sur le plan pénal, les États fédérés ne cherchaient pas à harmoniser le droit criminel, contrairement aux relations économiques ou encore aux questions postales, puisque les Américains considéraient ce domaine comme une « affaire locale ».

Il existe aux États-Unis une multiplicité de centres de décisions où l’ensemble des acteurs devaient tant bien que mal collaborer pour obtenir un système d’équilibres et de contrôles réciproques (*checks and balances*)¹²⁸, pour la protection des libertés des citoyens. Ainsi, les règles en matière de répression, aussi bien législative, matérielle, que territoriale, sont parsemées, lacunaires et n’excluent pas les chevauchements. Aussi, la centralisation de la décision répressive, à travers la police, la poursuite et la détermination de la culpabilité, est faiblement organisée et les décisions sont disparates. La participation des citoyens à l’œuvre de justice est encouragée. De manière générale, les Américains sont attachés, aussi bien en droit qu’en politique, au « couple libéralisme-décentralisation » et manifestent leurs inquiétudes, selon l’auteur, quant au fait qu’un pouvoir central à Washington se mette à commettre « des intrusions oppressives dans la vie et dans les libertés de ses citoyens »¹²⁹.

La crainte historique des Américains vis-à-vis d’une législation s’éloignant de cette culture libérale semble être justifiée. En effet, en obligeant les transporteurs aériens à transmettre les données personnelles des passagers aériens, le droit américain, alors engagé dans une « guerre contre le terrorisme »¹³⁰, a fait fi des considérations de protection des droits fondamentaux et a ainsi rompu avec une culture juridique qui prenait en compte le droit du justiciable américain et étranger (sous-section 1). À la suite des attentats du 11 septembre 2001, les États-Unis ont imposé aux compagnies aériennes desservant leur territoire de transmettre au

¹²⁷ J. CEDRAS, *Droit pénal américain*, Presses Universitaires de France, « Que sais-je ? », 1997.

¹²⁸ F. VERGNIOLE DE CHANTAL, « Les checks and balances à l’épreuve », in *L’impossible Présidence impériale. Le contrôle législatif aux États-Unis*, CNRS Éditions, 2016, en ligne à URL : <http://books.openedition.org/editions-cnrs/13531> consulté le 19 septembre 2023.

¹²⁹ J. CEDRAS, *Droit pénal américain*, Presses Universitaires de France, « Que sais-je ? », 1997.

¹³⁰ « La guerre contre le terrorisme » est l’expression qui résume l’approche du gouvernement de George W. Bush dans sa lutte contre le terrorisme après les attaques du 11 septembre 2001. V. P. J. SCHRAEDER, « La guerre contre le terrorisme et la politique américaine en Afrique », *Politique africaine*, n° 98, 2005, pp. 42-62.

ministère de la Sécurité intérieure américaine (DHS) les données PNR contenues dans leurs systèmes de réservation. Cette obligation, issue de l'Aviation and Transportation Act¹³¹, s'est appliquée dès le 5 mars 2003, sous peine d'interdiction d'opérer sur le sol américain. Le DHS a affirmé que ces données ont permis d'identifier environ 1750 cas suspects par an, jouant un rôle clé dans de nombreuses enquêtes antiterroristes¹³². D'autres pays ont adopté des systèmes PNR similaires. L'obligation de transmission imposée par le droit américain s'inscrit dans un environnement juridique où la protection des données personnelles et sectorielles est peu développée¹³³. Ceci offre une permissivité aux autorités américaines qui se soucient peu des considérations liées à la protection des droits individuels (sous-section 2).

Sous-section 1 – Une rupture dans le droit pénal américain

Les attentats du 11 septembre 2001 ont bouleversé l'approche juridique américaine qui tend désormais vers une marginalisation croissante des considérations liées à la protection des libertés fondamentales¹³⁴. Il s'agit d'une approche extraterritoriale du droit, nourrie par des visées de contrôle rigide des frontières. Or, cette extraterritorialité du droit américain interroge la légalité de l'action d'un État qui tente d'imposer ses lois hors de son territoire, autrement dit, au-delà de la limite « naturelle » de sa souveraineté¹³⁵.

Le rapport d'information déposé par la Commission des affaires étrangères et la Commission des finances de l'Assemblée nationale, en conclusion des travaux d'une mission d'information constituée le 3 février 2016 sur l'extraterritorialité de la législation américaine, distingue l'extraterritorialité d'édiction de l'extraterritorialité d'exécution¹³⁶. La première ne serait pas contraire aux principes de base du droit international tandis que la seconde le serait. Pour l'auteur du rapport, ce caractère de certaines législations américaines n'est pas fondé sur une

¹³¹ <https://www.congress.gov/bill/107th-congress/senate-bill/1447/text>.

¹³² P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

¹³³ La collecte des données PNR auprès des transporteurs aériens est prévue par la législation américaine 49 U.S.C. § 44909(c)(3) et ses règlements d'application à 19 C.F.R. § 122.49d.

¹³⁴ I. BECHROURI, « La 'guerre globale contre la terreur' : un discours contre-productif pour la lutte antiterroriste », *Les champs de mars*, n° 30, 2018, pp. 479-489. L'auteur rappelle que l'un des problèmes de l'approche antiterroriste américaine résidait dans le fait que l'ennemi désigné n'était pas proprement identifié au préalable.

¹³⁵ K. BERGER, « Le rapport d'information déposé par la commission des affaires étrangères et la commission des finances en conclusion des travaux d'une mission d'information », *Rapport d'information en conclusion des travaux d'une mission d'information constituée le 3 février 2016*, Assemblée nationale, 5 octobre 2016.

¹³⁶ L'extraterritorialité d'édiction consiste à édicter des normes tandis que l'extraterritorialité d'exécution consiste à appliquer le droit. Cela peut être par la contrainte mais elle est circonscrite au territoire de l'État qui édicte. La décision de la Cour permanente de justice internationale a jugé la compétence d'édiction conforme au droit international dans sa décision *Lotus* du 7 septembre 1927. Lire en ce sens J. KRANZ, « La notion de souveraineté et le droit international », *Archiv Des Völkerrechts*, vol. 30, no. 4, 1992, pp. 411-41.

revendication délibérée d'extraterritorialité mais sur des interprétations larges pour fonder sa compétence¹³⁷.

En principe, le droit d'un État s'applique sur son territoire, toutefois le droit américain semble avancer plusieurs types de justifications pour fonder une compétence juridictionnelle extraterritoriale. En droit américain, la compétence d'édicter des réglementations des États serait fondée, en droit coutumier et d'après une recension de jurisprudence détenant une certaine autorité aux États-Unis (les Restatements of the Law de l'American Law Institute) sur trois types de compétences. Tout d'abord, la compétence territoriale, qui peut inclure des faits survenus à l'étranger compte tenu de leurs effets sur le sol national (« théorie des effets »). Ensuite, la compétence personnelle existe pour tous les faits qui concernent les nationaux, y compris pour des faits survenant à l'étranger. Enfin, la compétence dite « réelle » inclut les atteintes à la sécurité nationale¹³⁸.

Par ailleurs, selon la troisième, et dernière, version du Restatement of Foreign Relations Law of the United States, § 402 et 403, le champ de compétences des États pour édicter des lois peut être fondé sur trois critères¹³⁹. Le premier critère est territorial et concerne, d'une part, les faits survenus pleinement ou pour une part substantielle sur le territoire national ou, d'autre part, sur la base de faits survenant hors du territoire mais ayant des effets substantiels sur le territoire. Le deuxième critère est un critère personnel, couvrant les activités, intérêts, statuts, relations des nationaux. Le troisième, un critère « réel », couvre les faits dirigés directement contre la sécurité de l'État ou éventuellement certains autres intérêts publics. Cette source de droit américain rappelle que la compétence juridictionnelle concernant des personnes ou activités ayant des connexions avec une autre juridiction étatique ne doit pas être exercée lorsque ce serait « déraisonnable » (*unreasonable*).

La doctrine juridique française semble admettre, sensiblement et de manière générale, les mêmes fondements de compétence qu'aux États-Unis. En effet, le droit français considère que la compétence est d'abord territoriale, mais peut aussi être justifiée par la nationalité ou des considérations de sécurité nationale, par exemple dans le cadre de la répression d'actes particulièrement graves comme ceux de terrorisme. Cette compétence est également admise dans le cas des nécessités de fonctionnement du service public, y compris à l'étranger. Ainsi,

¹³⁷ Le critère de compétence territoriale reprend le raisonnement selon lequel toute opération bancaire libellée en dollars, réalisée sur un autre territoire dans le monde, finit par donner lieu à une compensation effectuée sur le sol américain.

¹³⁸ Ibid.

¹³⁹ S. H. CLEVELAND, P. B. STEPHAN, « Introduction: The Roles of the Restatements in U.S. Foreign Relations Law », in *The Restatement and Beyond: The Past, Present, and Future of U.S. Foreign Relations Law*, New York, *Oxford Academic*, 22 octobre 2020.

le droit diplomatique affirme que les immunités de juridiction des diplomates doivent avoir pour contrepartie leur assujettissement aux juridictions de leur pays d'origine. La compétence est également « universelle » dans certains cas¹⁴⁰.

Le rapport de l'Assemblée nationale précité s'est penché sur la question de l'extraterritorialité pratiquée par les États-Unis alors que depuis quelques années, notamment à partir de 2008, il était observé une multiplication des pénalités financières infligées par ce pays à des entreprises étrangères, en très grande majorité européennes. Le rapport a mis en avant l'usage extensif et incertain de l'extraterritorialité américaine, qui crée des difficultés et que la justice américaine applique sans recours à des principes généraux de compétence territoriale ou personnelle, lesquels sont appliqués par tous les pays du monde, y compris la France¹⁴¹.

§ 1 – Le 11 septembre 2001 comme déclencheur d'une nouvelle approche juridique

Le développement de l'aviation civile durant le XX^e siècle s'est opéré dans le sillage d'une logique juridique définie par des États et à travers laquelle ces derniers ont très tôt affirmé leurs prérogatives de souveraineté¹⁴². Parmi ces prérogatives, on distingue la sûreté de la navigation aérienne dont l'État est garant. Ce dernier veille en particulier à la sûreté de l'aviation civile.

En dehors de quelques incidents isolés, la sûreté de l'aviation civile a rarement été mise en danger par les États eux-mêmes¹⁴³ mais plutôt par des actes criminels de groupes ou d'individus. Parmi ces actes les plus redoutés au XX^e siècle figure le terrorisme.

Le terrorisme aérien international a connu différentes phases liées aux événements qui ont marqué l'histoire des relations internationales. La question de la définition de la notion de terrorisme remonte à 1937, lorsqu'un premier texte international a été adopté sans qu'il n'entre cependant en vigueur¹⁴⁴. Plus récemment, en 2005, le Président de l'Assemblée générale de l'ONU a proposé, lors de la 59^e session, la définition suivante : « Toute action visant à causer la mort ou des blessures graves chez des civils ou des non-combattants, lorsqu'elle a pour objet, de par sa nature ou le contexte dans lequel elle s'inscrit, d'intimider une population ou de contraindre un gouvernement ou une organisation internationale à

¹⁴⁰ K. BERGER, « Le rapport d'information déposé par la Commission des affaires étrangères et la commission des finances en conclusion des travaux d'une mission d'information », Rapport d'information en conclusion des travaux d'une mission d'information constituée le 3 février 2016, *Assemblée nationale*, 5 octobre 2016.

¹⁴¹ Ibidem

¹⁴² O. CACHARD, « Le transport international aérien de passagers », *Les livres de poche de l'ADI*, LGDJ, 2015.

¹⁴³ Ibidem

¹⁴⁴ Il s'agit de la Convention sur la répression et la prévention du terrorisme, Société des Nations, Genève, 16 novembre 1937. Voir en ce sens. F. DUBUISSON, « La définition du 'terrorisme' : débats, enjeux et fonctions dans le discours juridique », *Confluences méditerranée*, 2017/3, (n° 102), pp. 29-45.

exécuter ou s'abstenir d'exécuter un acte quelconque, ne saurait être justifiée par aucun motif et constitue un acte terroriste »¹⁴⁵. Par ailleurs, en 2002, l'Union européenne a adopté la décision-cadre « relative à la lutte contre le terrorisme » qui liste une série d'infractions « terroristes » « relatives à un groupe terroriste » ou « liées à des activités terroristes »¹⁴⁶. Les Européens ont envisagé divers actes tels que l'atteinte à la vie et à l'intégrité physique, la prise d'otages ou la libération de substances dangereuses, lorsque l'auteur les commet dans le but de « gravement intimider une population » ou de « contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque », ou « gravement déstabiliser ou détruire les structures fondamentales, politiques, constitutionnelles, économiques ou sociales d'un pays ou une organisation internationale » (article 1 § 1).

Les attentats du 11 septembre 2001 ont vu les aéronefs se transformer en objets destinés à provoquer la terreur dans les airs ou sur le sol¹⁴⁷. Dans le domaine de la sécurité publique, il s'est alors produit un changement de paradigme : les déplacements des passagers aériens sont perçus comme un moyen pouvant faciliter la commission de crimes et, par ricochet, sont susceptibles de fragiliser la sécurité des États. C'est dans ce contexte particulier que les données des dossiers passagers sont devenues un outil de renseignement, de prévention et de lutte contre le terrorisme¹⁴⁸.

Avant les attentats du 11 septembre 2001, les données des passagers aériens avaient une visée plutôt commerciale. Leur utilisation n'a été possible qu'après l'invention, en 1959, du premier système de réservation informatique « Computer Reservation System (CRS) », dénommé SABRE¹⁴⁹. L'objectif de ce dernier était de garder une trace des flux d'information dans le domaine de l'aviation civile. Puis, en 1964, American Airlines et IBM ont entrepris une collaboration technique pour automatiser les processus de réservation et d'établissement des tarifs aériens¹⁵⁰. En 2024, il existe quatre principaux systèmes de réservation informatique : SABRE, Travelport (Galileo / Apollo), Travelport (Worldspan) et Amadeus. Les trois

¹⁴⁵ Projet de document proposé par le Président de l'Assemblée générale à la 59ème session, A/59/HLPM/CRP.1/Rev.2, du 10 août 2005, p. 21.

¹⁴⁶ Décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme, *J.O.*, L 164, 22 juin 2002, p. 3.

¹⁴⁷ O. CACHARD, « Le transport international aérien de passagers », *Les livres de poche de l'ADI*, LGDJ, 2015.

¹⁴⁸ Y. MAYAUD, « Répertoire de droit pénal et de procédure pénale », *Terrorisme – Prévention*, Dalloz, janvier 2018.

¹⁴⁹ E.M KUŞKONMAZ, “Privacy and Border Controls in the Fight against Terrorism”, *Immigration and Asylum Law and Policy in Europe*, Volume: 48, 18 mars 2021.

¹⁵⁰ V.CORREA, « Fasc. 978 : Données Des Passagers Aériens », LexisNexis, JurisClasseur Communication, 15 novembre 2019.

premiers sont basés aux États-Unis, tandis que le quatrième est basé dans l'Union européenne¹⁵¹.

Les données PNR, initialement à usage commercial, pouvaient être demandées par les autorités judiciaires dans le cadre d'une enquête ou d'une instruction. Toutefois, aucune législation n'obligeait alors les transporteurs et les agences de voyages à les transmettre aux autorités pour la prévention et la répression des infractions¹⁵².

Plus généralement, le droit pénal américain offrait une protection juridique aux citoyens américains, notamment contre les possibles abus de l'État. Cette protection juridique se fondait sur les règles constitutionnelles énoncées par la Cour suprême fédérale qui contraignaient les agents du pouvoir répressif. Le citoyen américain était jugé conformément à la garantie des droits constitutionnels de *due process of law* imposant notamment la présence d'un avocat de la défense et l'utilisation de méthodes proportionnées et connues à l'avance¹⁵³.

Les attentats 11 septembre 2001 ont engendré un choc émotionnel¹⁵⁴ sans précédent aux États-Unis et ailleurs. Les images de l'effondrement des célèbres *Twin Towers* ont imprégné la mémoire des Américains comme de tous les citoyens du monde. Le choc a été d'autant plus marquant à cause des moyens mis en œuvre pour commettre le crime : les passagers de l'aviation civile ont été victimes de l'attaque et en même temps transformés en moyens de commission de l'acte terroriste¹⁵⁵. Outre sa contre-attaque politique et militaire, l'administration américaine a mené une bataille dans le domaine du droit, dans le cadre de ce qu'elle a qualifié de « guerre contre le terrorisme »¹⁵⁶. Cette guerre s'est ainsi basée sur un arsenal législatif qui comprenait la détention secrète d'individus non-américains situés sur le territoire américain. Les individus capturés sur le territoire afghan ont en effet été transférés à Guantanamo, une base militaire extraterritoriale, et privés de conseils juridiques, des garanties

¹⁵¹ E.M KUŞKONMAZ, "Privacy and Border Controls in the Fight against Terrorism", *Immigration and Asylum Law and Policy in Europe*, vol. 48, 18 mars 2021.

¹⁵² S. SUTOUR et Y. DETRAIGNE, « Rapport n° 401 : La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives », *Sénat*, Commission des lois, 13 mai 2009, en ligne à URL : <http://www.senat.fr/ue/pac/E6014.html> consulté en ligne le 23 mars 2023.

¹⁵³ D.M. AMANN, « Le dispositif américain de lutte contre le terrorisme », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2000.

¹⁵⁴ F. CABASINO, « Les attentats du 11 septembre. Émotion et raison dans la presse en France et en Italie », *Mots. Les langages du politique*, 2004, pp. 21-33. V. G. FROMM, « Psychanalyse et trauma : retour sur le 11 septembre », *Diogenes*, n° 203, 2003, pp. 3-19. V. C. ANZIEU-PREMMEREUR, « Après le 11 septembre 2001 à New York », *Revue française de psychanalyse*, 2003, p. 865-876. V. France 24, « 11-Septembre : de Manhattan à Brooklyn, mémoires d'une journée en enfer », 9 septembre 2021, en ligne à URL : <https://www.france24.com/fr/am%C3%A9riques/20210909-11-septembre-de-manhattan-%C3%A0-brooklyn-m%C3%A9moires-d'une-journ%C3%A9e-en-enfer> consulté le 19 septembre 2023.

¹⁵⁵ Ibidem

¹⁵⁶ C. BUNZEL, "Jihadism on its own terms", *Hoover Institution Press*, 2017.

du droit constitutionnel américain et du droit international¹⁵⁷. La « guerre » du gouvernement américain, à travers l'installation de cette « zone de non-droit »¹⁵⁸, s'est étendue à toute personne présumée terroriste, citoyen ou non¹⁵⁹. Faisant souvent fi des frontières, l'arsenal législatif américain anti-terroriste s'est distingué dans le monde par la mise en place du système Passenger Name Record (PNR).

Le législateur américain a choisi de définir les dossiers passagers, les données PNR, en des termes généraux désignant les informations de réservation contenues dans le système de réservation électronique et/ou le système de contrôle des départs d'un transporteur aérien qui établissent l'identité et les plans de voyage de chaque passager ou groupe de passagers inclus dans le même dossier de réservation pour tout vol couvert¹⁶⁰. Cette définition extensive considère également le contenu des données PNR¹⁶¹ sachant que le transporteur aérien se voit obliger, sur demande, de fournir aux douanes un accès électronique à tous les éléments de données PNR relatifs à l'identité et aux projets de voyage d'un passager concernant tout vol, dans la mesure où le transporteur possède les éléments de données demandés dans son système de réservation et/ou système de contrôle des départs¹⁶².

Comme le rappelle le US Customs and Border Protection dans son Passenger Name Record (PNR) Privacy Policy¹⁶³, l'article 49 U.S.C § 44909 (c) (3) donne le droit aux autorités américaines de contrôle aux frontières de collecter les données PNR tandis que l'article 19 CFR § 122.49d détaille les principales exigences du système PNR américain. En général, les données des dossiers passagers sont exigées de tout transporteur, américain ou non, pour les

¹⁵⁷ D.M. AMANN, « Le dispositif américain de lutte contre le terrorisme », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2000.

¹⁵⁸ Ibidem

¹⁵⁹ M. OULD SLAHI, *Les carnets de Guantanamo*, Michel Lafon, 2015. Le citoyen mauritanien Mohamedou Ould Slahi a été détenu à Guantanamo pendant quatorze ans sans jamais être inculpé par la justice américaine. V. Amnesty International, « USA : Rendition – torture – trial? : The case of Guantánamo detainee Mohamedou Ould Slahi », 19 septembre 2006, Index Number: AMR 51/149/2006, en ligne à URL : <https://www.amnesty.org/en/documents/amr51/149/2006/en/> consulté le 19 septembre 2023.

¹⁶⁰ « Passenger Name Record (PNR) information refers to reservation information contained in an air carrier's electronic reservation system and/or departure control system that sets forth the identity and travel plans of each passenger or group of passengers included under the same reservation record with respect to any flight covered » (19 CFR § 122.49d, (b), (1))

¹⁶¹ Ibidem

¹⁶² « the air carrier, upon request, must provide Customs with electronic access to any and all PNR data elements relating to the identity and travel plans of a passenger concerning any flight under paragraph (a) of this section, to the extent that the carrier in fact possesses the requested data elements in its reservation system and/or departure control system » (19 CFR § 122.49d, (b), (2)).

¹⁶³ US Customs and Border Protection Passenger Name Record (PNR) Privacy Policy, US Department of Homeland Security, 21 juin 2013 https://www.cbp.gov/sites/default/files/documents/pnr_privacy_3.pdf

vols à destination ou au départ des États-Unis, y compris dans le cas où les passagers sont contrôlés ou inspectés dans l'État d'origine¹⁶⁴.

Le législateur américain prévoit de collecter, lorsqu'elles sont disponibles, les données des dossiers passagers suivantes¹⁶⁵ : l'identifiant unique PNR (« PNR record locator code »), la date de réservation ou de délivrance du billet, la date prévue pour le voyage, les noms et prénoms, les informations relatives au programme de fidélité, les autres noms figurant sur le PNR y compris le nombre de voyageurs, les informations de contact, les formes de paiement, l'itinéraire du voyage lié au PNR, l'identification de l'agence et de l'agent de voyage, les informations relatives à un éventuel partage de codes, les indications concernant la scission ou division du dossier passager (« split/divided PNR »), le statut de la réservation incluant la confirmation et l'enregistrement, les informations relatives au billet dont le numéro de billet et la classe tarifaire, aller simple le cas échéant, toutes les informations relatives aux bagages, le numéro de siège, les remarques générales, les informations SSR (« Special service request ») et OSI (« Other supplementary information »), les données API collectées et les changements apportés aux données PNR, autrement dit l'historique¹⁶⁶.

Cette longue liste reprend à l'identique les catégories que l'IATA (International Air Transport Association), l'OACI (International Civil Aviation Organization) et la WCO (World Customs Organization) identifient aujourd'hui dans leur liste de données de dossiers passagers¹⁶⁷. Certains chercheurs n'ont ainsi pas manqué de relever la redondance de cette longue liste de données personnelles¹⁶⁸. De son côté, l'IATA a regretté la multiplication des mécanismes de régimes nationaux de dossiers passagers, une situation qui fait peser sur les compagnies aériennes et les passagers certaines exigences qui ne sont pas forcément conformes aux standards internationaux¹⁶⁹. En effet, les autorités étatiques, notamment celles de l'immigration, des douanes ou de la police, ne se conforment pas toujours aux documents d'orientation adoptés par le secteur de l'aviation civile mais non contraignants¹⁷⁰.

¹⁶⁴ V.CORREIA, « Données des passagers aériens », *JurisClasseur Communication*, LexisNexis, 15 novembre 2019.

¹⁶⁵ Cette collecte des données PNR auprès des transporteurs aériens est prévue par la législation américaine 49 U.S.C. § 44909(c)(3) et ses règlements d'application à 19 C.F.R. § 122.49d.

¹⁶⁶ V.CORREIA, « Données des passagers aériens », *JurisClasseur Communication*, LexisNexis, 15 novembre 2019.

¹⁶⁷ WCO/IATA/ICAO API Contact Committee, Principles, Functional and Business Requirements – PNRGOV, oct. 2013, p. 11.

¹⁶⁸ V.CORREIA, « Données des passagers aériens », *JurisClasseur Communication*, LexisNexis, 15 novembre 2019.

¹⁶⁹ Ibidem

¹⁷⁰ Ibid.

Dans leur manière d'obtenir les données des dossiers passagers, les autorités américaines, à travers notamment l'article 19 CFR § 122.49d (c), ont choisi l'utilisation de la méthode « pull » exigeant des compagnies aériennes de donner accès à leur système de réservation électronique et/ou à leur Departure Control System (DCS)¹⁷¹ afin que leurs services de contrôle aux frontières puissent avoir accès aux informations des vols et les données concernant les passagers aériens. Cette méthode permet aux autorités compétentes de l'État membre, qui requièrent les données PNR, d'avoir un accès au système de réservation du transporteur aérien et d'en extraire une copie des données PNR requises. Ce n'est pas le cas de la méthode « push » qui implique, à l'inverse, que les transporteurs aériens transmettent eux-mêmes ces données à l'autorité requérante, ce qui leur permet de garder le contrôle sur les données transmises.

À l'intérieur du territoire américain, le droit local organise le transfert de ces données. En effet, les articles 19 CFR 122.49a, (e) et 19 CFR § 122.75a, (e) donnent le droit, au Service des douanes et de la protection des frontières, de transférer les données API et les manifestes de passagers reçus par voie électronique aux autres agences fédérales lorsque la protection de la sécurité nationale l'exige, qu'il s'agisse de passagers partant du territoire américain ou arrivant sur celui-ci. Les données PNR peuvent, de la même façon, être partagées avec d'autres agences fédérales mais uniquement dans le but de garantir la sécurité nationale (19 CFR § 122.49d, (d)). Le partage d'informations se fait conformément aux procédures établies par le département de la Sécurité intérieure (System of Records Notice – SORN) en tenant compte du droit applicable, notamment des accords internationaux conclus par les États-Unis dans ce domaine. Le département de la Sécurité intérieure tient à ce que les données des dossiers passagers ne puissent être transmises que de manière ponctuelle, lorsque des besoins spécifiques sont démontrés. La sécurité intérieure est ainsi assurée sous réserve que ces informations soient suffisamment protégées¹⁷².

Certaines données sont effectivement exclues de la collecte par les standards internationaux. Ainsi, le document 9944 de l'OACI précise que les États ne peuvent exiger de recevoir les données PNR des passagers que pour les seuls vols à destination, au départ ou en transit sur leur territoire, aussi bien pour les vols planifiés que pour ceux déroutés¹⁷³. Par ailleurs, le paragraphe 2.5.2 de ce document indique explicitement que les États ne doivent pas requérir des compagnies aériennes de fournir des données qui n'ont pas déjà été collectées dans leur

¹⁷¹ Ibid.

¹⁷² U.S. Department of Homeland Security, U.S. Customs and Border Protection Passenger Name Record Privacy Policy, 21 juin 2013, p. 4

¹⁷³ OACI, Guidelines on Passenger Name Record, § 2.6.1

système de réservation ou leur système de contrôle des départs (DCS). Selon la doctrine, les États les plus exigeants¹⁷⁴ se conforment à cette règle, même si peu de preuves existent démontrant que les États-Unis excluent bien ce type de données dans leur collecte. Le document 9944 indique également que les données des dossiers passagers ne doivent pas contenir d'informations non-nécessaires à la réalisation du vol¹⁷⁵ telles que l'origine ethnique, les convictions religieuses ou politiques, l'appartenance à des syndicats ou partis politiques, le statut marital et l'orientation sexuelle.

Cette nouvelle législation américaine s'est donc inscrite dans un contexte politique marqué par une tension sécuritaire croissante¹⁷⁶. Elle expose le citoyen américain à une collecte de ses données personnelles, donc au risque de violation de ses droits fondamentaux et, *in fine*, de son intimité¹⁷⁷. Ces données sur les passagers aériens permettent de suivre leurs déplacements afin de prévenir les actes criminels et terroristes, en facilitant l'exploitation et le croisement des informations via les systèmes informatiques aéroportuaires. Les actions terroristes sont souvent facilitées par les déplacements de leurs auteurs. Le caractère international de leur entreprise et la mobilité qu'elle suppose leur permet de s'assurer une clandestinité dans leur agissements¹⁷⁸.

Par conséquent, les données des passagers aériens constituent, pour le gouvernement américain, un outil de renseignement redoutable et efficace puisqu'elles permettent de briser les réseaux criminels. Toutefois, des voix critiques se sont élevées pour pointer du doigt les dangers que pourrait constituer l'utilisation de ces données¹⁷⁹ : le législateur ne délimite pas la durée de la conservation de ces données, l'instance chargée de les traiter n'est pas réellement

¹⁷⁴ V.CORREIA, « Données des passagers aériens », *JurisClasseur Communication*, LexisNexis, 15 novembre 2019.

¹⁷⁵ OACI, Guidelines on Passenger Name Record, § 2.1.9.

¹⁷⁶ D. SABBAGH, « Sécurité et libertés aux États-Unis dans l'après-11 septembre : un état des lieux », *Critique internationale*, n°19, 2003, pp.17-23, en ligne à URL : <https://www.cairn.info/revue-critique-internationale-2003-2-page-17.htm> consulté le 19 septembre 2023.

¹⁷⁷ Sur les pratiques qui relèvent plus spécifiquement du « profilage ethno-racial » (racial/ethnic profiling) – comme la convocation de quelque 8000 ressortissants étrangers originaires du Moyen-Orient et d'Afrique du Nord par l'Immigration and Naturalization Service (INS) à partir du mois de novembre 2001 –, nous pouvons citer D. SABBAGH, « Vers une relégitimation du “profilage ethno-racial” ? », *Critique internationale*, n° 14, janvier 2002, pp. 33-38; V. aussi S. ASHAR, « Immigration enforcement and subordination: the consequences of racial profiling after September 11 », *Connecticut Law Review*, n° 34, 2002, pp. 1185-1199, S. AKRAM ET K. JOHNSON, « Race, civil rights, and immigration law: after September 11, 2001 : the targeting of Arabs and Muslims », *New York University Annual Survey of American Law*, n° 58, 2002, pp. 295-355, ainsi que M. E. LEVEILLE, *Le profilage ethno-racial aux États-Unis : analyse juridique et historique avant et après le 11 septembre 2001*, mémoire de l'Institut d'études politiques de Paris, février 2003.

¹⁷⁸ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.

¹⁷⁹ S. SUTOUR et Y. DETRAIGNE, « Rapport n° 401 : La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives », *Sénat*, Commission des lois, 13 mai 2009, en ligne à URL : <http://www.senat.fr/ue/pac/E6014.html> consulté en ligne le 23 mars 2023.

indépendante, l'utilisation de données sensibles comme les opinions religieuses ou politiques qu'elles peuvent contenir.

La CNIL définit ces données sensibles comme « [des] informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale. Ce sont également les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique »¹⁸⁰.

Le ministère de l'Intérieur américain ne se base pas sur des critères précis s'agissant de son utilisation des données sensibles, car il considère que des informations pouvant être considérées comme sensibles peuvent être incorporées dans le transfert de données PNR. Or, ces données PNR sensibles peuvent inclure certaines informations révélant l'origine raciale ou ethnique, la religion ou la santé du passager. Le Customs and Border Protection (CBP), autorité en charge des douanes de la protection des frontières aux États-Unis, explique utiliser¹⁸¹ des filtres électroniques pour masquer automatiquement les données PNR identifiées comme sensibles qui ne peuvent ainsi être incluses dans le PNR lorsqu'elles sont transférées des systèmes de réservation et/ou de départ des transporteurs aériens vers le CBP. Les autorités américaines affirment que ces informations ne sont ni utilisées ni vues par le personnel du CBP, sauf dans des circonstances exceptionnelles impliquant que la vie d'un individu soit en danger ou gravement compromise, auquel cas des mesures préventives et supplémentaires seront prises.

§ 2 – Une nouvelle organisation des agences sécuritaires américaines

Après que le passager aérien a fourni ses données personnelles au moment de la réservation de son titre de transport, les données des dossiers passagers sont stockées dans les bases de données des systèmes de réservation mis en place par les agences de voyages et les compagnies aériennes. Ces données sont ensuite exploitées par le ministère de l'Intérieur américain (DHS)¹⁸², plus précisément le CBP¹⁸³.

¹⁸⁰ Cnil, « Les données sensibles c'est quoi ? », 2023, en ligne à URL : <https://www.cnil.fr/fr/cnil-direct/question/une-donnee-sensible-cest-quoi> consulté le 27 mars 2023.

¹⁸¹ Voir www.cbs.gov/travel/pnr.

¹⁸² C.FÉRAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », *Praxis CyberDroit*, Dalloz, 2020-2021.

¹⁸³ US Department of Homeland Security, "US Customs and Border Protection Passenger Name Record (PNR) Privacy Policy", 21 juin 2013 en ligne à URL : https://www.cbp.gov/sites/default/files/documents/pnr_privacy_3.pdf consulté le 27 mars 2023.

Bien que sa mission prioritaire soit « d'empêcher les terroristes et les armes terroristes d'entrer » sur le territoire américain, le CBP est également chargé de faire « respecter les douanes, l'immigration, l'agriculture et d'autres les lois américaines à la frontière, tout en facilitant également la circulation du commerce et des voyageurs »¹⁸⁴. Le ministère de l'Intérieur américain a également, depuis la mise en place des accords PNR, la responsabilité principale de la collecte des enregistrements des données PNR et utilise activement ces informations au niveau opérationnel. Le CBP est chargé de mettre en œuvre les politiques anti-terroristes après que le DHS a défini les politiques concernant le traitement de ces données. Ensuite le CBP collecte, utilise et diffuse les données PNR conservées dans l'ATS-P, système automatisé de stockage de ces données.

Selon le CBS¹⁸⁵, le but de la collecte d'informations PNR, avant l'arrivée ou le départ du voyageur, est d'aider ses agents à mesurer le risque associé à ce dernier lorsqu'il se déplace vers, depuis ou via les États-Unis. La collecte doit également permettre au CBP de prendre des décisions précises et complètes concernant les voyageurs, en exigeant une potentielle inspection supplémentaire en se fondant sur le droit applicable et les informations reçues. Le CBS met en avant deux avantages pour le voyageur dans la collecte de ses informations à l'avance¹⁸⁶ : d'une part, cela donne au CBP suffisamment de temps pour rechercher des correspondances possibles avec des enregistrements dérogatoires afin d'éliminer les résultats faussement positifs ; d'autre part, cela accélère le voyage en permettant au CBP d'effectuer des contrôles obligatoires avant l'arrivée d'un vol aux États-Unis, plutôt que d'obliger le voyageur, ainsi que tous les autres passagers du vol, à faire la queue pendant que leurs données sont collectées manuellement.

Concrètement, les dossiers passagers suivent un parcours rythmé en six étapes dès lors qu'ils sont élaborés par les autorités américaines¹⁸⁷, notamment le Customs and Border Protection. Ce processus commence avec une première étape consistant à programmer les systèmes du CBP pour accepter les PNR envoyés par un transporteur aérien ; jusqu'à 96 heures avant le départ d'un vol et toutes les modifications ultérieures apportées au PNR avant l'heure du vol

¹⁸⁴ US Department of Homeland Security, "A Report On The Use And Transfer Of Passenger Name Records Between The European Union And The United States", 26 juin 2015 en ligne à URL : https://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf consulté le 27 mars 2023.

¹⁸⁵ U.S. Customs and Border Protection, Passenger Name Record (PNR), 2023, en ligne à URL : <https://www.cbp.gov/travel/clearing-cbp/passenger-name-record> consulté le 27 mars 2023.

¹⁸⁶ Ibidem

¹⁸⁷ US Department of Homeland Security, "Report On The Use And Transfer Of Passenger Name Records Between The European Union And The United States", US Department of Homeland Security, 26 juin 2015 en ligne à URL : https://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf consulté le 27 mars 2023.

ou pour recevoir des mises à jour envoyées à des heures programmées. Si le CBP doit extraire des données, il le fait au plus tôt 96 heures avant le départ prévu.

La deuxième étape consiste en un filtrage du PNR non formaté contenant toutes les informations, y compris les données « sensibles ». Ce dernier est consulté puis filtré pour enlever les termes et codes « sensibles ». Des symboles sont placés à l'endroit où les termes et codes « sensibles » ont été supprimés et le PNR d'origine est filtré.

Ensuite, vient la troisième étape consistant en un filtrage du PNR pour les catégories de données approuvées indiquées dans le SORN ATS¹⁸⁸. Les éléments restants du PNR sont supprimés par le CBP et ne sont pas accessibles via le système. Les termes et codes sensibles sont supprimés et ne peuvent pas être recréés après 30 jours.

La quatrième étape est celle de la dépersonnalisation : après six mois, les données PNR sont dépersonnalisées. Des catégories spécifiques ne peuvent être repersonnalisées que par des utilisateurs désignés après avoir reçu l'autorisation d'un superviseur via le système. Le PNR lié à une mesure d'exécution spécifique ne sera pas dépersonnalisé pendant la durée de vie du dossier d'exécution.

La cinquième étape intervient cinq ans après la date de chargement initial du PNR : les données du PNR passeront à un statut dormant et non opérationnel, à l'exception du PNR lié à une mesure d'exécution spécifique, qui demeure disponible tout au long de la vie du dossier.

Enfin, la sixième étape intervient 15 ans à compter de la date de réception indiquée dans le dossier, le PNR sera entièrement anonymisé sans possibilité de repersonnalisation, à l'exception du PNR lié à une mesure d'exécution spécifique, qui sera disponible pendant toute la durée de l'exécution.

Outre le CBP, deux autres institutions américaines utilisent des données des passagers aériens. Il s'agit, d'une part, du *DHS Privacy Office* dont la mission principale est de protéger la vie privée des citoyens américains. La loi impose la transparence de toutes les activités du DHS. Ce bureau supervise les politiques de protection des données personnelles et la politique qui donne accès aux informations. Il est également légalement tenu d'évaluer toutes les nouvelles technologies utilisées par le ministère et leur impact sur la vie privée.

Le DHS Privacy Office est également amené à rédiger des rapports au Congrès sur ces questions ainsi que sur les plaintes concernant d'éventuelles violations de la vie privée. En outre, le DHS Privacy Office est responsable de la mise en œuvre d'initiatives en matière

¹⁸⁸ Automated Targeting System (ATS) System of Records Notice (SORN).

d'éducation et de formation liées à la protection de la vie privée pour plus de 240 000 employés du DHS. Ainsi, le DHS Privacy Office avait été amené à envoyer un expert à l'équipe de négociation des États-Unis pour l'Accord PNR de 2011.

D'autre part, le DHS Privacy Office dispose d'un bureau politique en charge de la coordination des initiatives prises et de la mise en place de la stratégie du ministère : the DHS Office of Policy. Ce bureau sert également de principal conseiller international auprès du ministère et, à ce titre, coordonne l'engagement multilatéral et bilatéral du DHS. Il examine, surveille et, le cas échéant, négocie les accords et arrangements internationaux¹⁸⁹ pour assurer la cohérence avec le plan et les stratégies d'engagement international du DHS.

Parallèlement à cette nouvelle configuration qui a été mise en place pour traiter les données personnelles des passagers aériens, le droit américain prévoit plusieurs moyens par lesquels les individus peuvent corriger des informations détenues par le DHS¹⁹⁰.

Une première est la possibilité de demander des modifications d'informations sachant qu'un voyageur peut solliciter une copie du dossier par le biais d'un processus décrit sur le site du CBS. L'objectif est de lui permettre de déterminer quelles informations se trouvent réellement dans son dossier PNR. Les demandes de modification doivent être conformes aux exigences de la loi américaine, en mentionnant le nom complet du demandeur, son adresse, ainsi que sa date et son lieu de naissance. Le demandeur doit motiver sa demande et respecter des conditions de forme. Un centre d'informations mis en place par le CBS peut être contacté par téléphone, via internet et par courrier.

Les voyageurs peuvent également demander réparation par le biais du programme du DHS : DHS Traveller Redress Inquiry Program (DHS TRIP), notamment celles et ceux qui pensent avoir été indûment refusés à l'entrée, ou refusés à l'embarquement pour le voyage ou identifiés pour une inspection supplémentaire par le CBP. Ces derniers peuvent soumettre une demande de réparation via ce programme, qui se veut être un guichet unique pour les personnes qui ont des questions ou cherchent à résoudre des difficultés rencontrées lors de

¹⁸⁹ A.D GIVENS, N. E. BUSCH, D.A. BERSIN, « Going Global: The International Dimensions of U.S. Homeland Security Policy », *Journal of Strategic Security*, 11, n° 3, 2018, pp. 1-34, en ligne à URL : https://digitalcommons.usf.edu/jss/vol11/iss3/2/?utm_source=digitalcommons.usf.edu%2Fjss%2Fvol11%2Fiss3%2F2&utm_medium=PDF&utm_campaign=PDFCoverPages consulté le 23 septembre 2023.

¹⁹⁰ U.S. Customs and Border Protection, Passenger Name Record (PNR), 2023, en ligne à URL : <https://www.cbp.gov/travel/clearing-cbp/passenger-name-record> consulté le 27 mars 2023. Voir : U.S. Department of Homeland Security, "DHS Can Strengthen Its International Cybersecurity Programs" OIG-12-112, 2012, pp.12-14, en ligne à URL <https://www.hsdl.org/?view&did=722620> consulté le 23 septembre 2023. Voir également : The White House, "Fact Sheet: U.S.-EU Cyber Cooperation", Office of the Press Secretary, 2014, en ligne à URL : <https://obamawhitehouse.archives.gov/the-pressoffice/2014/03/26/fact-sheet-us-eu-cyber-cooperation>, consulté le 23 septembre 2023.

leur contrôle dans les centres de transports ou au passage des frontières américaines. Ce programme est présenté comme un programme permettant à un voyageur de demander la correction de données erronées stockées dans le système ATS et d'autres données stockées dans d'autres bases de données DHS via une seule application. Les demandes de réparation DHS TRIP peuvent être faites en ligne ou via courrier.

La deuxième possibilité est le recours devant le Chief Privacy Officer. Dans le cas où une plainte ne peut pas être résolue par le CBP ou par le processus DHS TRIP, la plainte peut en effet être adressée au Chief Privacy Officer. Le droit américain prévoit que le chef de la protection des données personnelles américain doit consulter et étudier la plainte et y répondre. Conformément à la loi sur la sécurité intérieure de 2002, le responsable de la protection de la vie privée du DHS est statutairement obligé de veiller à ce que les informations personnellement identifiables soient traitées d'une manière conforme à la loi en vigueur. Ce dernier exerce une surveillance concernant la mise en œuvre de l'Accord de 2011¹⁹¹ pour en assurer le strict respect par le DHS et vérifier que des garanties appropriées sont mises en place. Les plaintes reçues des États membres de l'Union européenne au nom d'un résident européen, dans la mesure où ce résident autorise l'organe responsable à agir en son nom, doivent être traitées de manière accélérée¹⁹².

La troisième possibilité, un recours judiciaire initié par les voyageurs, quelle que soit leur nationalité, peut être possible dans les circonstances suivantes.

Premièrement, dans le cas d'un traitement incorrect de leurs données sachant que le Computer Fraud and Abuse Act (CFAA) (18 USC § 1030) permet aux individus d'intenter une action civile devant les tribunaux en vue d'obtenir des dommages-intérêts et un remboursement des frais d'avocat, lorsque leurs données personnelles, détenues dans un système informatique du gouvernement américain, y compris le système de ciblage automatisé (ATS) qui inclut le PNR, ont été traitées de manière incorrecte, leur causant ainsi un préjudice.

Deuxièmement, dans le cas d'une consultation, d'une divulgation, d'une communication ou d'une interception de manière incorrecte étant donné que l'Electronic Communications Privacy Act (18 USC § 2701 et suiv. et 18 USC §2510 et suiv.) permet à toute personne d'intenter une action civile devant un tribunal pour l'obtention de dommages-intérêts et le remboursement des frais irrépétibles, lorsque les données personnelles sont consultées ou

¹⁹¹ Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure, Bruxelles, 14 décembre 2011.

¹⁹² V. MITSILEGAS, « Coopération antiterroriste États-Unis/Union européenne : l'entente cordiale », *Au nom du 11 septembre... Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, 2008, p. 118-130.

divulguées de manière inappropriée, ou lorsque les communications filaires, orales ou électroniques de cette personne sont interceptées ou divulguées de manière inappropriée.

Troisièmement, dans le cas d'un ordre de transports particuliers, dès lors que la disposition 49 USC § 46110 autorise une personne concernée par des ordres de transports particuliers d'intenter un recours judiciaire auprès de la cour d'appel américaine, y compris des ordres qui mettent en œuvre les listes de surveillance de la DHS Transportation Security Administration.

Quatrièmement, dans le cas d'agissement arbitraire, abusif, contraire à la loi ou dépassant le domaine, l'Administrative Procedure Act (5 USC §§ 551 - 559) prévoit un contrôle judiciaire de l'action d'une agence qui a agi au-delà de son domaine d'activité. Le tribunal peut annuler une action administrative non conforme aux lois, arbitraire ou un abus de pouvoir discrétionnaire. Les particuliers peuvent déposer des réclamations APA en leur propre nom ou dans le cadre d'un recours collectif.

§ 3 – Un ordre juridique américain basé sur l'extraterritorialité

La nouvelle législation PNR américaine, comme le Patriot Act¹⁹³, la justice d'exception¹⁹⁴ et la tristement fameuse prison cubaine Guantanamo, caractérisent, depuis 2001, un nouveau dispositif américain contre le terrorisme. Cette prison, basée au Cuba, a matérialisé l'un des traits particuliers de cette riposte américaine sur le plan juridique : l'extraterritorialité. Des photographies d'hommes cagoulés, enchaînés, amaigris et à genoux près de cages ont suscité l'émoi de l'opinion publique internationale¹⁹⁵. La société civile à travers le monde, comme aux États-Unis, a critiqué cet arsenal législatif¹⁹⁶ qui remettait en cause l'engagement américain à respecter les droits de l'Homme, et *in fine*, a affaibli son « autorité morale dans le monde »¹⁹⁷.

¹⁹³ L'acte réglementaire de 2001, désigné par le sigle « PATRIOT », a étendu les pouvoirs de l'Attorney général sur les écoutes clandestines, s'appliquant également aux conversations auparavant confidentielles entre les prisonniers et leurs avocats.

¹⁹⁴ Des juristes américains parmi les plus renommés n'ont pas hésité à cautionner par avance les formes les plus extrémistes de rupture avec les principes de l'État de droit ; ainsi, Alan Dershowitz, professeur à la Harvard Law School et avocat reconnu pour ses prises de position « progressistes », en est venu à justifier explicitement l'usage de la torture pour les terroristes présumés lorsque les circonstances l'exigeraient. Voir A. Dershowitz, *Why Terrorism Works: Understanding the Threat, Responding to the Challenge*, New Haven, Yale University Press, 2002.

¹⁹⁵ J. MASTERS, « Guantanamo Bay: Twenty Years of Counterterrorism and Controversy », *Council on Foreign Relations*, 5 octobre 2021, en ligne à URL : <https://www.cfr.org/article/guantanamo-bay-twenty-years-counterterrorism-and-controversy> consulté le 27 mars 2023.

¹⁹⁶ D. COLE ET J. DEMPSEY, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*, New York, New Press, 2002, p. 149.

¹⁹⁷ J. GOLDSMITH ET C. SUNSTEIN, « Military tribunals and legal culture : what a difference sixty years make », *Public Law and Legal Theory Working Paper* n° 27, 2002, p. 14, en ligne à URL: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=12361&context=journal_articles consulté le 19 septembre 2023.

Ces images ont également poussé la société civile à appeler au respect de la Troisième Convention de Genève¹⁹⁸ qui prévoit qu'une Haute Partie contractante se doit de traiter de façon humaine les prisonniers de guerre en leur accordant des procès équitables, conformes à la Convention, en respectant leur droit de ne pas répondre aux questions au-delà de simples renseignements sur leur identité, en les libérant et en permettant leur rapatriement en fin de conflit. Or, les États-Unis ont refusé d'appliquer cette Convention considérant que les détenus en question n'étaient pas des prisonniers de guerre¹⁹⁹. Ainsi, l'ambassadeur américain en charge des crimes de guerre a affirmé que les dispositions de la Convention, bien qu'utiles en cas de traditionnels conflits interétatiques, étaient dépassées dans le cadre de la « nouvelle » lutte contre le terrorisme²⁰⁰. D'autres personnalités politiques américaines, formant une coalition de conservateurs et de libéraux américains, ont appelé au réexamen de cet « assaut contre la vie privée individuelle » après le 11 septembre²⁰¹.

Malgré cela, le Patriot Act²⁰² a fait son chemin au sein du droit américain alors que sa section 215 prévoyait que la collecte et la surveillance des communications pouvaient se faire sans mandat ni ordonnance judiciaire. Cette loi a en effet permis une surveillance à grande échelle des communications mondiales, qui a été dévoilée avec l'« affaire Prism », lorsqu'un journaliste américain du Guardian²⁰³ a révélé sur son blog le 5 juin 2013 que la National Security Agency (NSA) avait un accès illimité aux données de Verizon, l'un des principaux opérateurs américains de téléphonie et d'accès internet. Cette révélation s'appuyait sur des informations confidentielles livrées par l'informaticien américain²⁰⁴ travaillant pour différents sous-traitants de la NSA. Ce dernier a également révélé que neuf des plus grands acteurs

¹⁹⁸ Convention de Genève relative au traitement des prisonniers de guerre, 12 août 1949.

¹⁹⁹ D.M. AMANN, « Le dispositif américain de lutte contre le terrorisme », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2000.

²⁰⁰ V.K. SENGUPTA, « Geneva Conventions are outdated, say US envoy », *Independent* (London), 22 février 2022, p. 1, en ligne à URL : <https://www.independent.co.uk/news/world/americas/geneva-conventions-are-outdated-says-us-envoy-9194166.html> consulté le 27 mars 2023.

²⁰¹ S. MILLIGAN, « A Federal Push on Security Stirs a Bipartisan Bid to Guard Privacy », *Boston Globe*, 8 avril 2002, p. A1.

²⁰² Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act), 25 octobre 2001. Lire en ce sens. FINNEGAN ABDOLIAN, H. TAKOOSHIAN, « The USA Patriot Act: Civil Liberties, the Media, and Public Opinion », 30 *Fordham Urb. L.J.* 1429, 2003, en ligne à URL : <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2097&context=ulj> consulté le 23 septembre 2023. Voir également : B. HACKETT, « Covering (Up) the War on Terrorism: The Master Frame and the Media Chill », *Campaign for press & broadcasting freedom*, 2001.

²⁰³ G. GREENWALD, « NSA Prism program taps in to user data of Apple, Google and others », *The Guardian*, 7 juin 2013. Pour une étude, lire : K. WAHL-JORGENSEN, L. BENNETT, G. TAYLOR, « The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Revelations », *International journal of communication* 11, Cardiff University, UK, 2017, pp. 740-762, en ligne à URL : <https://dspace.loyno.edu/jspui/bitstream/123456789/121/1/Sinha.pdf> consulté le 23 septembre 2023.

²⁰⁴ D. LELOUP ET M. SZADKOWSKI, « Prism, Snowden, surveillance : 7 questions pour tout comprendre », *Le Monde*, 2 juillet 2013. Dans ce contexte, lire : D. P. FIDLER, *The Snowden Reader*, Indiana University Press, 2015, en ligne à URL : <http://www.jstor.org/stable/j.ctt16gh840> consulté le 23 septembre 2023.

d'internet (Apple, AOL, Facebook, Google, Microsoft, PalTalk, Skype, Yahoo et YouTube) auraient permis au Federal Bureau of Investigation (FBI) et à la NSA d'avoir directement accès aux données de leurs utilisateurs, grâce au système Prism, qui existe depuis 2007²⁰⁵.

Cette collecte illégale de données de communications de millions d'individus, en violation des droits fondamentaux de millions de citoyens²⁰⁶, a mis la lumière sur le hiatus existant entre Américains et Européens quant à leur conception de l'utilisation des données et de l'information. En effet, tandis que les premiers organisent un profilage à grande échelle dans un objectif sécuritaire, les seconds montrent leur indignation face à une telle atteinte aux droits fondamentaux des citoyens, en particulier le droit à la protection de leurs données personnelles.

La vice-présidente de la Commission européenne en charge de la Justice et des droits fondamentaux a d'ailleurs réagi de manière explicite en indiquant qu'« il est clair que les droits fondamentaux des citoyens ne sont pas négociables »²⁰⁷. À la suite de cette crise, une enquête a été initiée par le Parlement européen sur la base d'auditions de représentants des autorités américaines, de la Commission européenne et du Conseil. Il a également été convenu de réunir une commission d'experts des États-Unis et de l'Union européenne afin d'aborder la question de Prism et la protection des droits fondamentaux des citoyens européens²⁰⁸.

Par ailleurs, le G29 (groupe de travail « article 29 » sur la protection des données), regroupant les autorités de contrôle européennes, soucieux d'évaluer l'impact du programme Prism a adressé, le 13 août 2013, une lettre à la vice-présidente de la Commission dans l'objectif d'obtenir des clarifications sur la législation américaine en matière de surveillance des citoyens européens²⁰⁹. Toutes ces réactions expriment l'ampleur de l'incompréhension des deux côtés de l'Atlantique, qui semble résulter de divergences à la fois idéologiques et politiques.

²⁰⁵ E. MACASKIL, « NSA paid millions to cover Prism compliance costs for tech companies », *The Guardian*, 23 août 2013. Voir S. VON SOLMS, R. VAN HEERDEN, « The consequences of Edward Snowden NSA related information disclosures », Conference: 10th International conference on Cyber Warfare and Security ICCWS, Sukuza, South Africa, 2015, en ligne à URL : https://www.researchgate.net/publication/275019554_The_Consequences_of_Edward_Snowden_NSA_Related_Information_Disclosures consulté le 23 septembre 2023.

²⁰⁶ G.A. SINHA, « NSA surveillance since 9/11 and the human right to privacy », *Loyola Law Review*, 2013, en ligne à URL : <https://dspace.loyno.edu/jspui/bitstream/123456789/121/1/Sinha.pdf> consulté le 24 septembre 2023.

²⁰⁷ S. PEYROU, « De l'accord PNR à Prism, bilan et perspectives sur les malentendus transatlantiques : lutte anti-terroriste versus protection des données personnelles », *GDR-ELSJ*, 11 septembre 2013.

²⁰⁸ Ibidem

²⁰⁹ Ibid.

Le Patriot Act a été suivi par des amendements du Foreign Intelligence Surveillance Act de 1978 (FISA)²¹⁰, dont la section 702 autorise le gouvernement à collecter des informations à partir des communications entre son territoire national et l'étranger²¹¹. Le FISA a instauré une Cour spéciale, Foreign Intelligence Surveillance Court (FISC), dont les onze juges fédéraux, choisis par le Chief Justice, statuent dans le cadre d'une procédure non contradictoire, à huis clos, afin de valider les requêtes des services de renseignement vis-à-vis des seuls citoyens américains. Cette « Cour suprême parallèle » selon le New York Times²¹² a été critiquée pour son lien étroit avec le pouvoir exécutif américain. À la suite de l'affaire Prism, l'ancien président américain Barack Obama a promis de modifier le Patriot Act, ainsi que la Cour spéciale mise en place par le FISA, tout en déclarant : « vous ne pouvez pas avoir 100 % de sécurité, et aussi 100 % de respect de la vie privée, et zéro inconvénient. Nous avons des choix à faire en tant que société »²¹³.

Au sein des Constitutions européennes prévaut une logique plus favorable à la protection des droits fondamentaux ; l'approche du dossier PNR en est l'illustration. Les personnalités européennes ont ainsi vivement réagi à l'affaire Prism, que ce soit la Commission par la voix de sa vice-présidente, le Parlement européen, qui a instauré une commission d'enquête, et le G29 qui a publiquement manifesté son inquiétude en saisissant la Commission. Comme conséquence de cette « rupture anthropologique (...) par le fait de notre condition de toute part interconnectée »²¹⁴, la doctrine plaide pour un « habeas corpus numérique » qui viendrait compenser l'érosion des libertés publiques du fait de la politique antiterroriste. L'Union européenne, attachée à la défense des droits fondamentaux, dispose d'atouts concrets et importants pour faire avancer diverses réformes favorables à la protection des données à caractère personnel face au droit américain²¹⁵.

Fondé sur la sécurité, ce nouvel arsenal législatif anti-terroriste paraît bien dépasser sa raison principale lorsqu'il permet de détenir des individus qui sont en l'espèce des prisonniers non-citoyens américains, en dehors du territoire des États-Unis, donc loin des tribunaux internes.

²¹⁰ Les amendements apportés par le FISA Amendments Act de 2008, notamment la section 702, ont élargi les pouvoirs de surveillance du gouvernement américain, permettant la collecte sans mandat de communications électroniques entre des cibles étrangères et des personnes aux États-Unis.

²¹¹ S. M. SMYTH, *Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control*, New York, Routledge, 2019. Voir également : J. S. GRANICK, *American spies: modern surveillance, why you should care, and what to do about it*, Cambridge University Press, 2017.

²¹² S. PEYROU, « De l'accord PNR à Prism, bilan et perspectives sur les malentendus transatlantiques : lutte anti-terroriste versus protection des données personnelles », *GDR-ELSJ*, 11 septembre 2013. Lire en ce sens: R. MILLER, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, Cambridge University Press, 2017.

²¹³ Ibidem

²¹⁴ Ibid.

²¹⁵ Ibid.

Ainsi, Diane-Marie Amann a discerné une envie d'isoler ces individus dans une « zone de non-droit », où l'envie « est nourrie par cette colère qui l'emporte sur la présomption d'innocence et d'autres droits dont un individu bénéficie en tant qu'être humain »²¹⁶.

À cette colère s'est ajoutée une défiance vis-à-vis des institutions américaines. Le gouvernement, porteur de ce nouvel arsenal législatif, craint que « la procédure des Cours fédérales aboutisse à une remise en cause du poids et de la fiabilité des preuves présentées » tout comme le Gouvernement craint que « les juges américains, dont les postes à vie garantissent une vraie indépendance du pouvoir »²¹⁷ se tiennent au respect des exigences constitutionnelles de *Fundamental fairness* et du *Due process* plus qu'à l'obsession sécuritaire du gouvernement américain.

Enfin, un climat intellectuel et culturel a visiblement préparé l'opinion publique depuis quelques années à accepter cette vision du monde et de la justice. La représentation de « l'Orient », empreinte de préjugés, a été dès 1978 dénoncée par l'intellectuel américain Edward Saïd, celle-ci ne servant *in fine* que des agendas politiques²¹⁸. Le professeur de littérature comparée a ainsi rappelé l'imaginaire de l'Oriental que les Occidentaux pouvaient retrouver dans la culture de masse : « Le cinéma et la télévision associent l'Arabe soit à la débauche, soit à une malhonnêteté sanguinaire. Il apparaît sous la forme d'un dégénéré hypersexué, assez intelligent, il est vrai, pour trame des intrigues tortueuses, mais essentiellement sadique, traître, bas. (...) En parlant, il fait une grimace suggestive : c'est une image dégradée du cheikh de Valentino qui est en circulation »²¹⁹. Cette représentation de l'altérité a un impact sur le droit d'un accusé qui vient de la partie de la planète qui est ainsi incriminée.

Cette vision du monde, associée à un climat délétère, a abouti, deux mois après les attentats, à la mise en place par le président de l'époque d'une innovation judiciaire pour traiter les individus capturés en Afghanistan : la création de tribunaux d'exception. Son vice-Président de l'époque a justifié cette mesure par le fait que les terroristes « ne méritent pas les mêmes garanties et sauvegardes qu'un citoyen américain subissant le processus judiciaire normal »²²⁰. Cette nouvelle justice à deux vitesses n'eût été possible sans un fondement critiquable : une vision impérialiste du monde où l'Autre - l'Oriental - est regardé comme

²¹⁶ D.M. AMANN, « Le dispositif américain de lutte contre le terrorisme », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2000.

²¹⁷ Ibidem

²¹⁸ E. W. SAÏD, *Orientalism*, Pantheon Books, 1978.

²¹⁹ Ibidem

²²⁰ P. SLEVIN, G. LARDNER JR., « Bush Plan for Terrorism Trials Defended », *Washington Post*, 15 novembre 2001.

inférieur. Sur le plan juridique, un certain nombre d'universitaires et d'experts sont allés jusqu'à justifier la torture, au nom de la lutte contre le terrorisme²²¹. Sur le plan politique, cette approche du monde a mené aux pratiques dégradantes qui se sont déroulées à la prison d'Abu Ghraib, quelques années plus tard²²².

Pour Régis Debray, cette américanisation n'est que l'énième répétition de la longue histoire de l'humanité, d'une civilisation qui se déploie à travers l'exportation de sa culture, comme l'illustre l'exemple de l'Empire romain²²³. Les concepts juridiques se diffusent à travers la culture, comme en témoignent les primaires françaises inspirées des *primaries* américaines avant les élections présidentielles. Le droit devient un vecteur culturel pouvant transcender les frontières nationales et exercer une influence hégémonique. Ainsi, « l'universel, c'est le local sans les murs » pour reprendre les mots de Miguel Torga²²⁴. L'américanisation n'est pas un fait singulier mais le particulier américain qui devient universel.

En effet, loin d'être seulement une puissance militaire, politique et économique, les États-Unis n'ont pas assuré leur hégémonie sans une « offre » culturelle : « Pour en revenir au noyau dur - le radical irradiant -, la force militaire, condition nécessaire mais non suffisante, doit s'augmenter impérativement d'un imaginaire pour enflammer les cours, d'un entrepôt pour remplir les ventres et d'un magistère pour occuper l'esprit. L'imposition par la force, armée ou financière, ou les deux, resterait impuissante sans le rayonnement d'un code symbolique, seul à même, de faire un ensemble avec des morceaux »²²⁵. Or le droit américain semble bien faire partie de cet « ensemble » culturel qui intègre également une langue, des modes de vie et des goûts. Si l'on suit la logique de Debray, le droit américain dans son expansion vers l'Europe ne serait peut-être que la traduction d'un aspect d'une hégémonie qui dans d'autres circonstances a fait l'objet de moins de résistance.

D'ailleurs, la pression n'est pas toujours la cause principale d'une influence américaine sur le droit européen. En fait, américanisation ne signifie pas forcément impérialisme juridique. Parfois, et l'exemple du droit de la concurrence l'atteste, ce n'est pas la pression politique qui est le facteur déterminant mais plutôt « une conjonction d'intérêts entre les grandes entreprises

²²¹ A. VAN BRUNT, « The 'torture' memos prove America's lawyers don't know how to be ethical », *The Washington Post*, 12 décembre 2014.

²²² Human Rights Watch, *The Road to Abu Ghraib*, IV. Iraq: Applying Counter-Terrorism Tactics during a Military Occupation, 8 juin 2014.

²²³ R. DEBRAY, *Civilisation, Comment nous sommes devenus américains*, Gallimard, coll. Blanche, 2017, p.32

²²⁴ M. TORGA, *L'universel, c'est le local moins les murs*, William Blake, 2010.

²²⁵ R. DEBRAY, op. cit.

et le législateur [qui] a accéléré la réception de la réglementation (par ex., par l'*insider trading*) »²²⁶.

Pour autant, il convient de relever l'influence de la culture juridique américaine sur le droit contemporain qui se fait à travers les organisations internationales ; c'est notamment le cas de l'ONU qui a repris les notions dégagées par l'Administration Obama sur les sujets de lutte contre le terrorisme, en employant notamment le concept de « *countering violent extremism* »²²⁷ (CVE) dans les résolutions du Conseil de sécurité, que les acteurs internationaux et nationaux ont ensuite repris dans leurs travaux. Ce concept permet de rester en ligne avec le droit international qui refuse d'essentialiser la violence politique et d'associer le terrorisme ou l'extrémisme violent à une quelconque religion ou ethnie. Ce concept est venu remplacer un autre, idéologiquement très marqué, de « guerre contre le terrorisme » promu par le président américain George W. Bush²²⁸.

Cette terminologie, initiée par l'Administration Obama, de lutte contre le terrorisme²²⁹ a été reprise par le Conseil de sécurité des Nations Unies et par la plupart des institutions internationales luttant contre le terrorisme comme le Forum mondial de lutte contre le terrorisme (Global Counterterrorism Forum, GCTF) ou le Fonds mondial pour l'engagement de la communauté et la résilience (Global community engagement and resilience fund, GCERF). L'Administration Obama visait ainsi « les individus qui appuient ou commettent une violence motivée idéologiquement dans une visée politique ».²³⁰

C'est dans ce contexte que le Conseil de sécurité a voté le 15 décembre 2015 la résolution 2253 par laquelle les États membres ont été appelés à collecter les données des passagers aériens pour empêcher le retour des combattants terroristes étrangers. Le Conseil de sécurité a en effet explicitement exhorté « les États membres à coopérer pour empêcher les terroristes de recruter des éléments et pour faire front à la propagande et à l'incitation à l'extrémisme violent qu'ils diffusent sur Internet et dans les médias sociaux, notamment en formulant un contre-discours efficace, dans le respect des droits de l'homme et des libertés fondamentales et conformément aux obligations découlant du droit international, et souligne l'importance de

²²⁶ A. N. MARTIN, « Américanisation ou européanisation du droit pénal économique ? », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2006 p. 767.

²²⁷ C. BUNZEL, « Jihadism on its own terms », *Hoover Institution Press*, 2017.

²²⁸ R. DWORKIN, R. ROBERT, & M-O. PADIS, « George W. Bush, une menace pour le patriotisme américain », *Esprit*, 2002, pp. 6-23, en ligne à URL: <http://www.jstor.org/stable/24279185> consulté le 19 septembre 2023.

²²⁹ F. DUBUISSON, « La définition du "terrorisme" : débats, enjeux et fonctions dans le discours juridique », *Confluences méditerranée*, n° 102, 2017, pp. 29-45.

²³⁰ C. BUNZEL, *Jihadism on its own terms*, *Hoover Institution Press*, 2017.

la coopération avec la société civile et le secteur privé à cet égard »²³¹. Depuis 1999, l'adoption de termes américains s'était généralisée, notamment avec la résolution 1267 du Conseil de sécurité des Nations unies. Cette résolution, opérant sous le chapitre VII de la Charte des Nations unies, avait établi l'un des trois Comités du Conseil dédiés à la lutte contre le terrorisme international, ciblant spécifiquement Al-Qaïda, les talibans, ainsi que les individus et organisations affiliés à ces groupes.

Les Nations Unies ont pu, ainsi, bâtir un arsenal législatif international contre le terrorisme²³² et son financement. Les résolutions du Conseil de sécurité n'ont cessé de demander aux États membres de prendre des mesures nécessaires et appropriées, conformément à leurs obligations, afin d'interdire la commission d'un acte terroriste et de prévenir un tel comportement.

Sous-section 2 – Une conception intrusive des dossiers passagers

Centré sur l'aspect économique et peu investi dans la protection des libertés individuelles, le droit américain des données personnelles offre donc peu des garanties pour la protection de ces dernières. Dès lors, une telle conception du droit peut revêtir parfois un caractère intrusif en ce qu'elle est susceptible de porter atteinte au droit à la vie privée d'une personne²³³. Cette approche juridique laisse le champ large aux autorités américaines s'agissant du traitement des données personnelles des passagers aériens.

§ 1 – Une conception faible et sectorielle américaine de la protection des données personnelles

Le droit américain de la protection des données personnelles se distingue par une myriade de mesures sous la forme de lois sectorielles relatives à la vie privée et aux données personnelles, à la fois fédérées et fédérales²³⁴, qui se sont multipliées ces dernières années. Cette architecture juridique différente du volet du droit des données personnelle explique, en partie, la différence d'approches entre l'Union européenne et les États-Unis en matière de protection des données à caractère personnel, même si depuis le 11 septembre 2001 une certaine convergence semble avoir lieu.

²³¹ Conseil de sécurité, résolution 2253, S/RES/2253 (2015).

²³² D. DUEZ, « De la définition à la labellisation : le terrorisme comme construction sociale », in K. BANNELIER, T. CHRISTAKIS, O. CORTEN ET B. DELCOURT, *Le droit international face au terrorisme*, Paris, Pedone, 2012, p. 116.

²³³ Définition, Intrusif, *Usito*, Le dictionnaire de l'Université de Sherbrooke.

²³⁴ S. LE STRUJON, « Le California Consumer Privacy Act : premier pas vers un RGPD américain ? », *Revue de l'Union européenne*, Dalloz, 2020.

La notion de *privacy*, traduite sommairement en français par « vie privée », est historiquement considérée comme trouvant son origine dans la *common law*, quand bien même le Bill of Rights ou la Constitution des États-Unis ne mentionnent pas explicitement le droit au respect de la vie privée²³⁵. Le *right to privacy*, traduit par le droit au respect de la vie privée, est identifié et défini par Samuel Warren et Louis Brandeis comme « the right to be let alone »²³⁶. Ce concept a été développé de manière limitée par la jurisprudence de la Cour Suprême des États-Unis²³⁷ qui a établi certaines garanties du respect de la vie privée des premier, troisième, quatrième, neuvième et quatorzième amendement de la Constitution.

Toutefois, cette dernière s'est toujours montrée réticente à consacrer de manière explicite le droit à la protection des données personnelles en tant que droit autonome garanti par elle²³⁸. Les juges américains se sont bien plus volontiers attachés à consacrer la *physical privacy* ou la *decisional privacy* que ce droit à la protection des données personnelles. Par conséquent, aux États-Unis, le système juridique reconnaît un droit fondamental à la vie privée²³⁹ mais il est manifeste que ce droit devient plutôt nébuleux dans le domaine de la confidentialité des informations²⁴⁰. Ainsi, le fondement juridique du droit à la protection des données personnelles souffre d'une certaine fragilité. Il n'existe pas aux États-Unis de cadre légal de portée générale pour le traitement des données personnelles, ni aucune agence nationale indépendante de contrôle.

Au niveau fédéral américain, le Privacy Act de 1974 régit les données personnelles collectées par le gouvernement, le Health Insurance Portability and Accountability Act (HIPAA) porte sur les données de santé, le Gramm-Leach-Bliley Act (GLBA) encadre les données du secteur financier, ou encore le Children's Online Privacy Protection Act (COPPA) régule la collecte de données sur les enfants en ligne²⁴¹. Ces législations sectorielles déterminent donc un régime de protection des données selon leur nature ; ainsi, certaines données spécifiques, comme les données financières ou de santé, bénéficient d'une protection élevée. Pour les

²³⁵ A. ADAM, « L'échange de données à caractère personnel entre l'Union européenne et les États-Unis », *Revue de droit européen*, Dalloz, 2006, p. 411.

²³⁶ L. BRANDEIS, S. WARREN, "The Right to Privacy, the implicit made explicit", *Harvard Law Review*, 15 décembre 1890.

²³⁷ Affaire *Roe v. Wade*, 410 US 113, 1973.

²³⁸ A. ADAM, « L'échange de données à caractère personnel entre l'Union européenne et les États-Unis », *Revue de droit européen*, Dalloz, 2006, p.411.

²³⁹ *Ibidem*

²⁴⁰ « The legal system recognizes a fundamental right of personal privacy, but it is clear that this right becomes rather nebulous in the area of informational privacy ».

²⁴¹ S. LE STRUJON, « Le California Consumer Privacy Act : premier pas vers un RGPD américain ? », *Revue de l'Union européenne*, 2020.

autres données, les entreprises peuvent les exploiter librement à la condition de ne pas faire preuve de « pratiques déloyales ».

Par ailleurs, une loi générale sur la protection des consommateurs contre les pratiques déloyales a été votée. Son application est contrôlée par l'Agence fédérale pour la protection des consommateurs (FTC), laquelle a développé une véritable « *common law* » relative aux données personnelles des consommateurs. Contrairement au paradigme européen qui protège la donnée en tant que composante de la vie privée de l'individu et comme droit fondamental, le paradigme américain de la protection des données personnelles se distingue par une conception économique de la donnée, axée autour de la protection du consommateur dans le cadre d'un système économique. Au sein de l'Union européenne, le débat sur l'État de droit - les droits qui en découlent dont ceux de la protection de la vie privée et des données personnelles - caractérise l'identité du citoyen européen qui s'est développée depuis la fin de la Seconde guerre mondiale. Ce défi constitutionnel est vital pour la survie du projet européen.

Au contraire, le paradigme américain de protection des données personnelles peut être qualifié de sectoriel et réactif, et s'en remet à l'autoréglementation²⁴². La doctrine y voit la conséquence « d'une méfiance atavique envers toute réglementation étatique » mais « ce type d'explication n'est, dans le meilleur des cas, que partiel, et dans le pire des cas, trompeur »²⁴³. Paradoxalement, c'est aux États-Unis que le débat public sur la protection des données personnelles est d'abord apparu.

Le législateur américain aurait même pu faire des États-Unis le premier État démocratique à se doter d'une législation en la matière. En effet, un rapport du ministère de la Santé américain de 1973 posait déjà certains principes de protection des données : la transparence, la finalité, la qualité, l'intégrité et la sécurité des données²⁴⁴. Il est frappant de constater que ces principes ne sont pas si différents de ceux que l'on retrouve aujourd'hui dans la directive européenne relative à ce sujet. D'ailleurs, ce rapport aurait pu servir de base à la création d'une législation globale et aurait alors permis à ce que les positions européenne et américaine soient bien plus aisément compatibles.

Aujourd'hui, cette divergence tend à se réduire grâce à l'initiative de certaines législations fédérées. Historiquement pionnier en matière de législation relative à la vie privée, le

²⁴² Ibidem

²⁴³ J. RULE, « La protection des données personnelles aux États-Unis : la réaction à la directive européenne », *Revue française d'administration publique*, janvier-mars 1999.

²⁴⁴ A. ADAM, « L'échange de données à caractère personnel entre l'Union européenne et les États-Unis », *Revue de droit européen*, 2006, p. 411.

législateur californien s'est distingué très tôt étant donné que, dès 1972, la Constitution californienne a été révisée pour intégrer le droit à la vie privée parmi les droits « inaliénables » de tous les citoyens. Depuis, cet État a adopté des mécanismes spécifiques pour protéger la vie privée de ses habitants, notamment l'Online Privacy Protection Act, la Privacy Rights for California Minors in the Digital World Law ou encore la Shine the Light Law visant à donner aux Californiens une méthode de questionnement vis-à-vis des entreprises traitant les renseignements personnels des consommateurs²⁴⁵.

Étant aujourd'hui un bastion des entreprises numériques friandes en données personnelles, l'État de la Californie a adopté le 28 juin 2018 le California Consumer Privacy Act (CCPA)²⁴⁶, entré en vigueur le 1^{er} janvier 2020. Ce texte a été présenté comme la loi américaine la plus proche du RGPD ; il s'agit ainsi d'un exemple de l'influence importance de législation européenne. Elle a transformé la vision de la protection de la vie privée aux États-Unis. Pour la doctrine, le CCPA illustre un effort sincère de la part des décideurs politiques américains pour renforcer les pouvoirs des consommateurs et adapter les lois à l'ère numérique²⁴⁷. Dans ses aspects les plus significatifs, le CCPA est similaire au RGPD²⁴⁸.

§ 2 – Une mise en avant de la lutte contre le terrorisme

La prise en charge de l'utilisation des dossiers passagers par le ministère de l'intérieur américain (Department of Homeland Security) et non pas par le ministère en charge des transports américains (Department of Transportation) démontre l'accent mis sur l'approche sécuritaire dans la construction du régime juridique du PNR américain qui n'intègre pas le souci de l'*equilibrium* européen entre sécurité collective et libertés individuelles. L'ancien secrétaire d'État (Under Secretary for Policy) du ministère américain des transports admet la controverse autour du PNR en ce qui concerne la protection des données personnelles, notamment avec l'Europe, mais continue de défendre le PNR américain qui s'inscrit dans le cadre de ce qu'il appelle « une grande stratégie » d'échange d'informations²⁴⁹.

Les transporteurs aériens se sont retrouvés dans l'obligation d'opérer des transferts de données de passagers vers des pays tiers sans assurer un niveau adéquat de protection et donc en infraction avec la directive 95/46. En effet, l'utilisation de ses données des dossiers passagers se veut avant tout et surtout répressive. Elle vise à lutter notamment contre le

²⁴⁵ S. LE STRUJON, « Le California Consumer Privacy Act : premier pas vers un RGPD américain ? », *Revue de l'Union européenne*, Dalloz, 2020.

²⁴⁶ California Consumer Privacy Act of 2018, CAL. CIV. CODE, § 1789.100 - 1789.199.

²⁴⁷ S. LE STRUJON, « Le California Consumer Privacy Act : premier pas vers un RGPD américain ? », *Revue de l'Union européenne*, Dalloz, 2020.

²⁴⁸ Ibidem

²⁴⁹ J. SHANE, « Air transport in crisis », *Revue de droit des transports*, n° 12, décembre 2008, entretien 1.

terrorisme et les crimes supranationaux comme le précise la législation américaine qui exige des compagnies aériennes opérant des vols à destination, en provenance ou via les États-Unis, de fournir au ministère de l'intérieur américain (Department of Homeland Security), à l'autorité en charge des douanes et de la protection des frontières (U.S. Customs and Border Protection), certaines données personnelles des passagers aériens, principalement à des fins de prévention, de détection, d'enquête et de poursuite des infractions terroristes et des crimes connexes et de certains autres crimes de nature transnationale²⁵⁰. Les autorités américaines ont tenu à souligner cela dès le premier paragraphe de leur politique relative à la protection de la vie privée (Privacy Policy)²⁵¹.

S'agissant du principal objectif donné à la collecte des dossiers passagers, les autorités américaines considèrent que celle-ci permettra aux agents postés à la frontière de mieux cerner celles et ceux à qui les autorités vont imposer une plus stricte inspection²⁵².

Cette précision faite, les autorités américaines rappellent l'utilisation des dossiers passagers pour lutter contre le terrorisme, le crime organisé et tout ce qui pourrait constituer une menace pour leur sécurité ou pour les besoins de la justice américaine²⁵³. Le but principal de la collecte de ces informations est de permettre aux autorités douanières et de protection des frontières de prendre des décisions précises et complètes sur les passagers nécessitant une inspection supplémentaire avant l'entrée au pays, sur la base des instructions des forces de l'ordre et d'autres informations.

²⁵⁰ La collecte des données PNR auprès des transporteurs aériens est prévue par la législation 49 U.S.C. § 44909(c)(3) et ses règlements d'application à 19 C.F.R. § 122.49d. « U.S. law requires airlines operating flights to, from, or through the United States to provide the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), with certain passenger reservation information, called Passenger Name Record (PNR) data, primarily for purposes of preventing, detecting, investigating, and prosecuting terrorist offenses and related crimes and certain other crimes that are transnational in nature » U.S. Customs and border protection, Receipt of Passenger Name Record (PNR) Data, https://www.cbp.gov/sites/default/files/documents/pnr_faq_3.pdf.

²⁵¹ US Customs and Border Protection Passenger Name Record (PNR) Privacy Policy, US Department of Homeland Security, 21 juin 2013 https://www.cbp.gov/sites/default/files/documents/pnr_privacy_3.pdf

²⁵² Ibidem

²⁵³ « The primary purpose for soliciting this information is to enable CBP to make accurate, comprehensive decisions about which passengers require additional inspection at the port of entry based on law enforcement and other information. DHS/CBP uses PNR strictly:

(1). To prevent, detect, investigate, and prosecute [...] a. Terrorist offenses and related crimes, including [...] b. Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature; [...]
2) on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court;
(3) to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.
(4) for domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR ».

Les autorités américaines compétentes utilisent les données des passagers aériens²⁵⁴ afin de prévenir, détecter, enquêter et poursuivre les infractions terroristes et crimes connexes ainsi que tous les autres crimes de nature transnationale passibles d'une peine d'emprisonnement de trois ans ou plus. Cela suppose une évaluation au cas par cas, lorsque nécessaire, en raison de menaces graves ou de risques pour la sécurité de toute personne, ou sur ordre d'un tribunal. L'objectif est d'identifier les individus susceptibles de subir un interrogatoire approfondi à leur arrivée ou à leur départ des États-Unis, pour faire respecter la loi nationale, les décisions judiciaires ou les procédures légales. Cette démarche est également entreprise pour détecter toute violation de la loi ou tout comportement suspect lors du traitement des données des passagers aériens. Avec cette approche extensive des dossiers passagers, les États-Unis octroient à leurs autorités des motifs qui justifient une utilisation de ces données dépassant le cadre anti-terroriste initialement pensé²⁵⁵, en consacrant des infractions aux contours imprécis.

En 2001, cette approche unilatérale et extraterritoriale²⁵⁶ de lutte contre le terrorisme, à travers l'utilisation des données personnelles des passagers aériens, a donné lieu à des oppositions. En France, la Cnil, l'autorité en charge de la protection des données personnelles, a considéré que ce système « pouvait porter une atteinte grave au respect de la vie privée et à la protection des données personnelles »²⁵⁷ avec un système qui cible un grand nombre de personnes et enregistre de très nombreuses informations.

À cette époque, la Cnil craignait que la communication des dossiers passagers aux autorités américaines puisse constituer un « détournement de finalité du traitement informatique », dès lors que ces données concernées sont collectées à l'origine « à des fins commerciales et non pour des raisons de sécurité »²⁵⁸. Cette inquiétude concernait également le niveau de protection de ces informations personnelles une fois traitées par les autorités américaines²⁵⁹.

²⁵⁴ US Customs and Border Protection Passenger Name Record (PNR) Privacy Policy, US Department of Homeland Security, 21 juin 2013 https://www.cbp.gov/sites/default/files/documents/pnr_privacy_3.pdf

²⁵⁵ B. E. ALTSCHULER, Review of American Surveillance: Intelligence, Privacy, and the Fourth Amendment, by A. GREGORY, *Political Science Quarterly*, 132(4), 2017, pp. 755–757, en ligne à URL : <http://www.jstor.org/stable/45175877> consulté le 23 septembre 2023.

²⁵⁶ M. P. GIBNEY, “The Extraterritorial Application of U.S. Law: The Perversion of Democratic Governance, the Reversal of Institutional Roles, and the Imperative of Establishing Normative Principles”, *Boston College International & Comparative Law Review*, 1996, en ligne à URL : <https://lira.bc.edu/files/pdf?fileid=63ad7b27-4fa1-4027-836c-3c67f6d8e464> consulté le 23 septembre 2023.

²⁵⁷ CNIL, « Système API-PNR : qu'en pensez la CNIL ? » <https://www.cnil.fr/fr/cnil-direct/question/le-systeme-api-pnr-quen-pense-la-cnil>.

²⁵⁸ C. FÉRAL-SCHUHL, Transfert des données à caractère personnel hors de l'Union européenne, *Praxis CyberDroit*, Dalloz, 2020-2021.

²⁵⁹ Ibidem

Cette inquiétude a des raisons historiques en Europe, notamment en France, dont la culture juridique européenne reste marquée par l'expérience tragique de la Seconde guerre mondiale. En effet, des personnes de la communauté juive ont pu être identifiées par les nazis, parce que ces derniers ont pu avoir accès aux données détenues par des sociétés privées²⁶⁰. Cette réticence ancrée dans la culture juridique européenne fonde les traditions constitutionnelles des États européens qui convergent vers une protection maximale en la matière.

§ 3 – Une réaction européenne minimaliste face une disposition sur les données PNR d'inspiration américaine

Impuissante face à ce défi posé par la législation américaine, la Cnil n'a pu que constater que les autorités européennes avaient concédé aux autorités américaines, en mars 2003, un accès direct aux systèmes de réservation des principales compagnies desservant les États-Unis²⁶¹. Cette concession a été faite sans que les autorités européennes puissent assurer à leurs citoyens une protection des données de leurs dossiers passagers comme le requièrent les législations de l'Union européenne sur la vie privée²⁶².

L'absence de réaction juridique européenne a pris fin avec la signature de l'accord de Washington le 28 mai 2004²⁶³ entre le ministère de l'Intérieur américain et la Commission européenne, après que le Conseil a mandaté la Commission, le 23 février 2004, pour négocier avec les autorités américaines. La Commission a soumis au Conseil, le 17 mars 2004, une proposition de décision²⁶⁴, soumise pour consultation au Parlement le 25 mars 2004. Le Conseil a finalement adopté, le 17 mai 2004, la décision 2004/496/CE portant conclusion de l'accord, qui est entré en vigueur le 28 mai 2004.

Ladite décision affirme que les données des passagers aériens transférées au Bureau des douanes et de la protection des frontières américain bénéficient d'un niveau de protection adéquat. Les Européens ont obtenu les garanties suivantes : un nombre plus réduit de données collectées et conservées par les autorités américaines (34 catégories de données sont transférées) ; les données sensibles permettant de révéler des indications sur la religion ou la santé ne sont plus transmises ou si elles le sont, sont filtrées et supprimées ultérieurement ; les données ne peuvent être utilisées que dans le cadre de la lutte contre le terrorisme et la grande

²⁶⁰ L. GRARD, Transfert de données personnelles des passagers, *Revue de droit des transports*, n° 9, septembre 2007, comm. 197.

²⁶¹ Ibidem

²⁶² Ibid.

²⁶³ Commission, décision 2004/535/CE 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique, *JOUE* L 235/11, 6 juill., p. 11.

²⁶⁴ (COM/2004/190 final).

criminalité et elles sont effacées après un délai maximal de trois ans et six mois, sauf pour les données consultées dans le cadre d'investigations spécifiques ; les autorités américaines informent notamment les passagers sur la finalité du transfert, des traitements et sur l'identité du responsable du traitement ; les personnes concernées disposent d'un droit d'accès et de rectification et les autorités chargées de la protection des données dans l'Union européenne ont compétence pour assister les personnes dans le cadre d'une plainte auprès des autorités américaines ; le tri des données ne peut être effectué par les autorités américaines qu'au cas par cas et pour des objectifs convenus et le transfert des données vers d'autres autorités gouvernementales américaines ou étrangères se fait au cas par cas et après notification à une autorité désignée au sein de l'Union européenne.

Comme le rappelle le chercheur Flavian Mariatte²⁶⁵, ce premier accord, qui reste déséquilibré au regard de la protection des données, a été conclu dans un contexte international sous tension. Les autorités européennes ont probablement pensé « qu'il était préférable de conclure rapidement un accord sans se montrer trop pointilleux, dans un premier temps, sur des exigences visiblement incompréhensibles outre-Atlantique au regard de l'enjeu, dans l'espoir d'une solution plus globale, multilatérale et équilibrée à terme ».

Le Conseil a rappelé dans sa décision précitée les deux motifs qui, selon lui, ont justifié la conclusion de cet accord : « la situation d'incertitude dans laquelle se trouvent les compagnies aériennes et les passagers » ainsi que la nécessité « de protéger les intérêts financiers des parties concernées ». En effet, le non-respect de la législation américaine exposait les compagnies à la privation du droit d'atterrissage et à des amendes de l'ordre de 5 000 \$. Les autorités américaines n'avaient pas caché que, faute de disposer des données sollicitées, elles intimeraient l'ordre au pilote d'un avion « douteux » de revenir à son point de départ, avec toutes les conséquences que cela emporte pour les passagers²⁶⁶.

Ainsi, pour différents acteurs concernés par l'initiative unilatérale américaine en matière de droit aérien, la conclusion d'un accord entre Américains et Européens permettait le maintien des relations transatlantiques et la conservation du bon déroulement des liaisons aériennes. Ces justifications et garanties ne sont toutefois pas apparues suffisantes pour les autres institutions européennes, notamment pour le Parlement européen, les États membres et la Cour de justice de l'Union européenne.

²⁶⁵ F. MARIATTE, « Protection des données personnelles des usagers des transports aériens », *Nouvelles technologies*, Europe n° 7, juillet 2004.

²⁶⁶ Ibidem

§ 4 – Le PNR comme symptôme d’une américanisation du droit

Le développement de l’arsenal répressif américain contre les drogues, le crime organisé ou le terrorisme mené par les États-Unis a été un facteur d’accélération de l’harmonisation de certains pans du droit international²⁶⁷. Contrairement au droit pénal économique, où les initiatives législatives qui mettent en mouvement l’harmonisation d’un domaine particulier proviennent des altérations dans l’économie internationale qu’il s’agit de corriger, découlant du processus de globalisation, l’américanisation du droit du PNR vient d’un événement spécifique, à savoir les attentats terroristes du 11 septembre 2001 qui se sont produits sur le sol américain même.

Historiquement, le droit de la concurrence européen a été le premier ensemble normatif à expérimenter l’influence du droit américain, à travers notamment le modèle Sherman Act dont la portée est extraterritoriale²⁶⁸. En effet, la délégation de compétence, à travers des sanctions pénales ou administratives, n’était pas commune dans les ordres juridiques européens à la fin de la Seconde guerre mondiale.

L’Allemagne est le premier pays européen à avoir été concerné par l’influence grandissante du droit anticoncurrentiel américain, par le biais de lois contre la concentration mettant fin à la structure des entreprises promue par le national-socialisme²⁶⁹. Plus tard, le droit européen de la concurrence est apparu pour la première fois dans le traité CECA, se donnant également pour objectif de mettre fin à la concentration existante, notamment des entreprises du bassin du Rhin, sous influence américaine visible « tant à travers des formes légales, que par les premières études doctrinales sur le droit de la concurrence »²⁷⁰. Le juriste espagnol Garrigues a décrit ce processus d’une façon très imagée en estimant que « le droit de la concurrence est venu en Europe dans le sac à dos des soldats américains »²⁷¹.

Aujourd’hui, cette américanisation concerne tout l’ordre juridique et, depuis presque vingt ans, de vastes secteurs du droit pénal. Par exemple, s’agissant de la politique américaine pénale de lutte contre la drogue, le terrorisme ou la criminalité organisée, de nombreux éléments de la Racketeer Influenced and Corrupt Organizations (RICO) Act (Lois sur les organisations motivées par le racket et la corruption) ont été repris à travers le monde et sont

²⁶⁷ A. N. MARTIN, « Américanisation ou européanisation du droit pénal économique ? », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2006, p. 767.

²⁶⁸ E. FRIEDEL-SOUCHU, « Extraterritorialité du droit de la concurrence aux États-Unis et dans la Communauté européenne », *Revue critique de droit international privé*, Dalloz, 1995.

²⁶⁹ A. N. MARTIN, « Américanisation ou européanisation du droit pénal économique ? », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2006, p. 767.

²⁷⁰ Ibidem

²⁷¹ J. GARRIGUES, *La defensa de la competencia mercantil*, Madrid, 1964.

devenus des prototypes d'un droit pénal globalisé, démontrant ainsi une américanisation du droit. Cette influence de la législation américaine se manifeste aussi dans des domaines du droit spécifique au contexte social et politique américain. En effet, le droit américain s'est surtout distingué dans sa lutte contre la criminalité « locale » comme le traitement de la délinquance sexuelle violente par le développement des mesures de neutralisation²⁷². En la matière, l'utilisation des données personnelles a été introduite pour lutter contre ce fléau, notamment dans la mise en place de fichiers des délinquants sexuels.

Par ailleurs, cette influence se distingue par l'utilisation d'un discours sécuritaire spécifique avec l'emploi d'une terminologie caractéristique, comme l'expression « tolérance zéro », et par la prolifération de systèmes de vigilance ou de sécurité privé, notamment les caméras de surveillance²⁷³.

Au-delà de l'existence de principes juridiques similaires des deux côtés de l'Atlantique, ce qui semble décisif dans ce phénomène d'américanisation est l'influence grandissante des nouvelles stratégies de politique criminelle telles que l'apparition d'autorités administratives avec des pouvoirs importants de sanction, la collaboration avec les instances chargées du contrôle qui échangent davantage sur la sanction et le rôle policier attribué à diverses administrations publiques, avocats ou audits de comptes.

Plus spécifiquement, des chercheurs américains, dont Robert Kagan, considèrent que l'américanisation du droit serait en train d'affecter l'axiologie de la culture juridique européenne²⁷⁴. Ainsi, l'*adversarial legalism*, un système dans lequel la solution des conflits se fait à travers la lutte d'adversaires dans le cadre d'un procès, avec un juge qui joue un rôle moins actif, a pris le pas sur l'importance de la loi et des administrations publiques comme outils essentiels pour la résolution des conflits sociaux (*burocratic legalism*). Les questions de territorialité et d'extraterritorialité qui découlent de la protection des données personnelles interrogent, en fin de compte, le droit international public. Le droit unilatéral dont se sont prémunis les États-Unis, en mettant des États souverains devant le fait accompli, a pu justifier des contre-mesures d'autres États lorsque la réalité politique le permettait.

Dans sa dénonciation de l'accord PNR, une députée européenne n'a pas hésité à critiquer cette politique juridique du fait accompli : « Les États-Unis mettent dans la balance la libéralisation des visas à destination des États-Unis et l'accès direct à de nombreuses bases de données, dont

²⁷² Ibidem

²⁷³ Ibid.

²⁷⁴ R. A. KAGAN, *Adversarial Legalism, The American Way of Law*, Harvard University Press, 9 janvier 2003.

le PNR²⁷⁵. Entre deux pays alliés, ce n'est pas une façon de faire ». La législation américaine extraterritoriale qui touche l'Europe n'est finalement que le prolongement d'un processus qui avait déjà touché les autres pays frontaliers puisque l'initiative « *secure flight* », utilisant le transfert de données de passagers aériens, avait inclus le Mexique et le Canada.

²⁷⁵ L. CHECOLA, « L'UE approuve le transfert aux USA des données des passagers européens », *Le Monde*, 19 avril 2012.

Section 2 – La contestation opposée par le droit européen

Contrairement aux États-Unis, l'Union européenne n'est pas encore une puissance mondiale puisqu'elle ne dispose pas des attributs traditionnels d'une puissance étatique dans les relations internationales²⁷⁶, dont le plus important est l'armée. Bien que le projet d'une armée européenne ait été abordé dans le cadre de la Communauté européenne de défense, dès 1954, aujourd'hui il n'existe pas à proprement parler d'armée européenne.

Toutefois, l'Union européenne a aujourd'hui la capacité de fonder sa projection internationale en se reposant sur un droit à portée mondiale. Cette nouvelle doctrine de l'extraterritorialité européenne, qui a été conceptualisée par Anu Bradford sous le terme de « Brussels Effect », permet à l'Union européenne d'avoir une influence dans les relations internationales grâce à la force attractive du marché européenne exercée à l'endroit d'opérateurs ou de consommateurs de pays tiers et à travers un droit caractérisé par une portée mondiale (*global reach*)²⁷⁷. Ainsi, ici, l'extraterritorialité européenne devient un vecteur de promotion des valeurs et des intérêts européens, en exigeant des sujets de droit des pays tiers, y compris du gouvernement américain, le respect de règles et standards extra-économiques européens, dont la protection des données personnelles des citoyens européens.

L'opposition aux mesures américaines de transmission des dossiers passagers par le droit européen a mis en avant la complexité des institutions européennes qui se sont exprimées, de manière variable, contre cet acte unilatéral américain à travers divers actes juridiques et déclarations politiques, sans que cela n'ait eu de conséquences juridiques décisives (sous-section 1). La frilosité européenne dans son opposition à l'hégémonie politico-juridique américaine est sous-tendue par un réalisme politique que les décideurs politiques européens ont mis en avant pour éviter un vide juridique (sous-section 2).

Sous-section 1 – Une contestation institutionnelle sans conséquences juridiques

Les institutions européennes ont émis des réserves vis-à-vis du projet PNR américain, allant d'avis à des décisions de justice condamnant les accords de transfert de données des passagers aériens. Toutefois, cette opposition s'est faite sous des formes éparses et variées, empêchant une position institutionnelle commune qui puisse rééquilibrer le rapport de force juridique jusqu'ici en faveur des Américains.

²⁷⁶ Banque de France, « Rapport sur l'extraterritorialité du droit de l'Union européenne », *Haut comité juridique de la place financière de Paris*, mai 2022 en ligne à URL : https://www.banque-france.fr/sites/default/files/rapport_46_f.pdf consulté en ligne le 28 février 2022.

²⁷⁷ A. BRADFORD, "The Brussels Effect. How the European Union rules the World", Oxford, Oxford University Press, 2020, p. 1.

§ 1 – Un accord critiqué mais confirmé par les institutions européennes

En plus de susciter de vives inquiétudes, la conclusion de l'accord euro-américain de 2004 a soulevé un concert de résistances, de mises en garde et de protestations des plus vigoureuses. En effet, dès le 24 octobre 2002, le G29 a rendu un avis dans lequel il s'alarmait sur la protection des données personnelles des citoyens européens²⁷⁸.

Ce même groupe a ensuite adopté deux autres avis²⁷⁹ intégrant l'évolution enregistrée au cours des négociations entre Européens et Américains. Les premiers projets d'accord ne l'avaient pas rassuré. Par ailleurs, le Parlement européen s'est explicitement opposé à la conclusion de cet accord à trois reprises, tout en invitant le Conseil, sans parvenir à un résultat concret, à soumettre le projet à la Cour de justice pour avis²⁸⁰. Le Parlement européen a continué de veiller au respect des droits fondamentaux par les autres institutions européennes en négociation avec les institutions américaines.

Le 30 mai 2006, la contestation de l'accord de 2004 par le Parlement européen, exprimant une crainte quant au niveau inadéquat de protection des données transférées aux États-Unis, a conduit la grande chambre de la Cour de justice à annuler la décision de conclusion de l'accord au motif de l'utilisation d'une base juridique erronée²⁸¹. Dans la même décision, la Cour a annulé la décision d'adéquation décidée par la Commission européenne sur le fondement de la directive « données personnelles » de 1995.

Pour donner suite à une convention intérimaire, un nouvel accord a été signé en juillet 2007 pour une durée de sept ans. Cet accord fut toutefois rejeté, en mai 2010, par le Parlement européen qui a ajourné son vote d'approbation sur ledit accord, bien que ce dernier ait été appliqué. Un nouvel accord a ensuite été signé, le 14 décembre 2011, finalement approuvé par le Parlement européen en avril 2012²⁸². Ces différentes séquences montrent que les

²⁷⁸ Groupe « Article 29 », Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis (11647/02/FR/Final).

²⁷⁹ Groupe « Article 29 », Avis 4/2003, du 13 juin 2003, sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers 11070/03/FR et Avis 2/2004 du 29 janvier 2004, sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (US CBP) (10019/04/FR), disponibles sur le site de la Commission.

²⁸⁰ Parlement européen, Rapport de la Commission des libertés et des droits des citoyens, de la justice et des affaires du 7 avril 2004, accompagné de l'avis de la Commission des affaires étrangères, des droits de l'Homme, de la sécurité commune et de la politique de défense des 5-6 avril 2004 (A5-0271/2004).

²⁸¹ CJCE, 30 mai 2006, aff.C-317/04 et C-318/04, Parlement c/Conseil : JurisData n°2006-400092 ; Rec. 2006, I, p. 4721. – V. V. Michel, La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration, *La revue trimestrielle de droit européen*, Dalloz, RTD eur. 2006, n°3, pp. 549-559.

²⁸² Décision 2012/472 du Conseil, 26 avril 2012, JOUE, no L 215, 11 août, relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure.

protestations institutionnelles n'ont pas permis d'exaucer la volonté des Européens de mettre en œuvre le transfert de données des dossiers passagers.

Après l'adoption par la Commission de la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers en 2011, le Contrôleur européen de la protection des données (ci-après CEPD) avait émis certain nombre d'observations le 11 novembre 2011, à la suite d'une consultation informelle.

Dans la continuité de ses avis et de ceux du G29, le 9 février 2012, le CEPD a rendu un avis²⁸³ plus complet sur les données PNR dans lequel il fait deux remarques d'ordre général. D'une part, en rappelant que la Charte des droits fondamentaux de l'Union européenne considère que « toute limitation des droits fondamentaux et des libertés ne peut être apportée que si elle est nécessaire, respecte le principe de proportionnalité et est prévue par la loi ». Or, dans le cas de l'accord euro-américain, « la nécessité et la proportionnalité des systèmes PNR et des transferts en masse de données PNR vers des pays tiers n'ont pas été démontrées jusqu'à présent ». D'autre part, le CEPD retenait les « quelques améliorations par comparaison avec l'accord de 2007 » et notait l'existence « des dispositifs de protection adéquats en termes de sécurité et de supervision des données » mais faisait remarquer « qu'aucune des principales préoccupations exprimées dans les avis précités, ni des conditions requises par le Parlement européen pour donner son consentement, n'ont été respectées ». Ces deux observations générales ont précédé des remarques plus particulières sur les manquements de l'accord vis-à-vis des droits fondamentaux européens sur la protection des données personnelles.

Malgré l'accueil favorable que le CEPD réserva finalement à l'accord, de nombreuses préoccupations subsistaient à ses yeux vis-à-vis de « l'approche globale de la question des données PNR, la limitation de la finalité, les catégories de données à transférer au DHS, le traitement des données sensibles, la période de conservation, les exceptions à la méthode « push », les droits des personnes concernées et les transferts ultérieurs ». Les préoccupations du CEPD s'inscrivaient dans une approche globale européenne qui souhaitait concilier la sécurité collective et les libertés individuelles. C'est pourquoi il conclut son avis en citant le Parlement européen dans sa résolution du 5 mai 2011 : « les principes de nécessité et de proportionnalité sont essentiels pour mener une lutte efficace contre le terrorisme ».

²⁸³ Avis du CEPD, 9 déc. 2011, sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure : JOUE n° C 35, 9 févr. 2012, p. 16, § 10.

§ 2 – *Un accord violant les standards européens de protection des droits fondamentaux*

Le contenu de l'accord a été jugé gravement attentatoire aux exigences européennes en matière de protection des droits fondamentaux en général, et en matière de protection des données à caractère personnel en particulier, affirmées à l'article 8 de la Charte des droits fondamentaux de l'Union européenne²⁸⁴. L'accord a soulevé des controverses car plusieurs violations ont été mis en exergue en matière de protection des données personnelles.

1. *Des finalités imprécises et extensives*

Bien que les données PNR sont collectées à des fins de lutte contre le terrorisme et la grande criminalité transnationale, la doctrine²⁸⁵ considérait que la formulation de l'article 4 de l'accord, faute de précision, était susceptible d'ouvrir la porte à une extension inadmissible de ses finalités. C'est le cas, par exemple, pour les infractions visées à l'article 4, paragraphe 1 b, passibles d'une peine d'emprisonnement d'au moins trois années, qui pourraient permettre d'utiliser les données PNR recueillies à d'autres fins comme pour la sécurité des frontières. L'extension des finalités concerne également le paragraphe 2 de l'article qui permet « l'usage des données PNR pour n'importe quelle finalité du moment que cet usage est, d'une manière ou d'une autre, décidé par une juridiction »²⁸⁶. Cette extension des finalités pour lesquelles les données sont collectées, dépassant les finalités initiales de lutte contre le terrorisme et la grande criminalité transnationale, ne peut plus répondre à l'exigence de nécessité imposée par la Charte des droits fondamentaux de l'Union.

2. *Des catégories de données transférées discutables*

Originellement, l'accord euro-américain de 2004 avait prévu 34 catégories de données PNR transférées. En 2007, le nouvel accord les a réduits à 19 mais la doctrine n'y a vu qu'un changement de forme²⁸⁷ au moment où l'accord de 2012 a été signé. Le CEPD a soutenu l'idée de réduction de la liste des données PNR transmises. Parmi les données transmises, les données sensibles sont celles qui l'ont le plus préoccupé étant donné que, selon les standards européens de protection des droits fondamentaux, celles-ci ne doivent pas être utilisées. Une exception demeure à l'article 6 de l'accord qui indique que leur usage est autorisé dans « des circonstances exceptionnelles » mais elles ne sont conservées que pendant un délai de trente jours, voire au-delà « pour une durée précisée dans la législation des États-Unis aux fins

²⁸⁴ P. GAIA, « La Charte des droits fondamentaux de l'Union européenne », *Revue française de droit constitutionnel*, n° 58, 2004, pp. 227-246.

²⁸⁵ S. PEYROU, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », *Droits fondamentaux, Europe, Revue Mensuelle LexisNexis Jurisclasseur*, juillet 2012.

²⁸⁶ Ibidem

²⁸⁷ Ibid.

d'enquêtes, de poursuites ou de mesures répressives spécifiques ». Le CEPD s'est toutefois explicitement prononcé contre le traitement de ces données sensibles.

3. *Une durée de conservation excessive*

Les délais de conservation des données sont un point central dans la contestation du point de vue américain sur ces accords car non seulement ils n'ont pas été réduits par rapport aux précédents, mais au contraire ils ont été allongés sans réel garde-fou.

En principe, les données recueillies sont conservées dans une base de données « active » pendant cinq ans maximum. Après six mois, les données PNR sont « dépersonnalisées et masquées ». Passé ce délai, les données sont transférées dans une base de données « dormante » pour dix années supplémentaires, où elles peuvent à tout moment être « repersonnalisées » dans le cadre « d'opérations menées par des services répressifs », en rapport avec « un cas, une menace ou un risque identifiable »²⁸⁸.

À l'issue de cette durée de quinze ans, les données conservées sont censées être entièrement « anonymisées ». Leur période de conservation est ainsi infinie. Or, dans la mesure où le risque de « repersonnalisation » des données existe, cette conservation sans limites apparaît comme manifestement disproportionnée, même au regard des objectifs visés par le texte. Par conséquent, elle contrevient aux exigences européennes en matière de protection des données²⁸⁹.

4. *Des modalités de transferts de données partiellement satisfaisantes*

Répondant aux critiques vis-à-vis de l'accord PNR de 2007, le nouvel accord a mis en place un transfert des données par la méthode « push »²⁹⁰. Toutefois, les paragraphes 4 et 5 de l'article 15 prévoient des exceptions qui permettent aux autorités américaines d'avoir un accès direct aux données par un système « pull »²⁹¹, méthode qui avait été précisément vivement critiquée par le G29²⁹².

²⁸⁸ Ibid.

²⁸⁹ Ibid.

²⁹⁰ Elle prévoit que les transporteurs aériens transmettent eux-mêmes les données des passagers à l'autorité requérante, ce qui leur permet de garder le contrôle sur les données transmises.

²⁹¹ Elle permet aux autorités compétentes de l'État membre, qui requièrent les données PNR, d'avoir un accès au système de réservation du transporteur aérien et d'en extraire une copie des données PNR requises.

²⁹² Lettre du 19 janvier 2011 du G29 adressée à la commissaire Madame Malmström, relative aux accords PNR avec les États-Unis, le Canada et l'Australie : « One of the main concerns yet to be addressed is that of the US authorities having direct access to PNR data in the EU by using terminals in their offices in the US, despite the existence of the push system. Through these terminals officials could pull data from the reservation systems of carriers and so access all the data on all the flights of a particular airline. There were no logs kept to show what data had been accessed. The Working Party has been informed that a filtering mechanism was to be put in place by November 2010 so that only data on US-related flights could be accessed. Although it has not had any further information on this filtering mechanism, the Working Party considers it fundamental that any future agreements

5. Une absence de garantie pour les transferts ultérieurs

L'accord a prévu un transfert ultérieur de données à des autorités nationales américaines ou à des États tiers s'il existe des garanties « comparables » en matière de respect de la vie privée. Or, la finalité pour laquelle ces données peuvent être transmises est sujette à débat pour deux raisons. D'une part, en cas de partage de données à l'intérieur des États-Unis, les finalités extensives, prévues à l'article 4 de l'accord, posent problème. D'autre part, si les données PNR d'un citoyen de l'UE sont transférées à un État tiers, les autorités compétentes de l'État dont il relève doivent désormais être informées – une avancée juridique certes – mais l'article 17 de l'accord PNR ne se prononce pas sur les finalités pour lesquelles de telles données peuvent être transférées. Par conséquent, ce vide ouvre la voie à un usage potentiellement abusif et incompatible avec les exigences européennes en matière de protection des données.

§ 3 – Des moyens de contrôle du respect de la protection de la vie privée insatisfaisants

L'accord euro-américain a prévu des procédures administratives de contrôle du respect des garanties en matière de protection de la vie privée, à l'instar des procédures judiciaires ouvertes aux particuliers pour défendre leurs droits, lesquelles manquent d'effectivité dans leur mise en œuvre.

L'accord PNR de 2012 a introduit des mécanismes de surveillance destinés à protéger la vie privée. Toutefois, ceux-ci ont été confiés à des agents ministériels chargés des questions de respect de la vie privée (dont le haut responsable de la protection de la vie privée au DHS « Chief Privacy Officer ») qui, par essence, ne peuvent être exempts « de toute influence extérieure, y compris celle émanant directement ou indirectement de l'État »²⁹³. Dès lors, ces nominations ne peuvent répondre aux conditions d'indépendance exigées par le juge européen²⁹⁴ en matière de protection de la vie privée.

En outre, l'article 14, paragraphe 2 de l'accord a instauré un mécanisme de surveillance confié au Bureau de l'inspecteur général du DHS, au bureau d'évaluation des programmes gouvernementaux et au Congrès américain. Toutefois, étant donné que ce contrôle peut être attribué à "une ou plusieurs des entités" mentionnées, il est possible qu'en pratique, il soit délégué uniquement à l'autorité relevant du DHS. Ainsi, aucun contrôle effectivement

provide for data to be pushed to the US authorities, with no possibility for US officials to separately access the data ».

²⁹³ S. PEYROU, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », Droits fondamentaux, Europe, *Revue Mensuelle LexisNexis Jurisclasseur*, juillet 2012.

²⁹⁴ B. STIRN, « L'indépendance du juge dans le cadre européen : évolutions et interrogations partagées », *Revue trimestrielle des droits de l'Homme*, n°125, 2021, pp. 5-13.

indépendant de l'accord PNR signé en 2012 entre les États-Unis et l'Union européenne n'est assuré.

Les mêmes doutes sont apparus s'agissant des procédures ouvertes aux personnes souhaitant faire valoir leurs droits. En effet, l'accord a prévu un droit de « recours judiciaire effectif, conformément au droit des États-Unis, indépendamment de sa nationalité, de son pays d'origine ou de son lieu d'origine »²⁹⁵. Or, ce droit n'indique pas pour autant qu'une procédure spécifique de recours existe en faveur des citoyens de l'Union européenne. L'article 13, paragraphe 3 de l'accord renvoie à un certain nombre de lois américaines susceptibles de fonder un recours judiciaire mais ne précise pas s'il confère de nouveaux droits aux citoyens de l'Union, en dehors de ceux dont les citoyens européens bénéficient de toute manière, indépendamment de l'accord. Cette imprécision sur les voies de recours a suscité des interrogations quant aux droits pouvant être revendiqués, dans la pratique, par les justiciables.

L'accord PNR entre les États-Unis et l'Union européenne a soulevé d'autres débats puisque le Privacy Act n'est pas applicable aux données PNR. En effet, l'article 21 de l'accord précise que celui-ci « ne crée ni ne confère, en vertu du droit des États-Unis, aucun droit ou avantage sur toute autre personne ou entité, privée ou publique ».

Par conséquent, de sérieuses questions se sont posées s'agissant de la volonté des autorités américaines de se conformer, comme elles le mentionnent pourtant, dans un délai raisonnable, aux requêtes de citoyens européens. En effet, un recours judiciaire introduit par un citoyen américain désirent obtenir des informations concernant ses données de dossiers passagers et n'ayant finalement obtenu qu'un nombre limité d'informations a nourri les craintes quant aux chances d'un citoyen européen d'obtenir satisfaction dans un cas semblable²⁹⁶. Pour sa part, le CEPD a conclu que le droit à un contrôle juridictionnel accordé par les États-Unis aux termes de l'accord « peut ne pas être équivalent au droit de recours effectif dans l'Union européenne, en particulier à la lumière de la restriction énoncée à l'article 21 »²⁹⁷.

Sous-Section 2 – Une contestation limitée par réalisme politique

L'absence de fermeté européenne face aux demandes américaines quant au transfert de données personnelles des passagers aériens, illustre la faiblesse du droit européen lorsque sont

²⁹⁵ Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au Ministère américain de la sécurité intérieure, Journal officiel n° L 0215 du 11/08/2012.

²⁹⁶ Affaire Hasbrouck c. US Customs and Border Protection, citée in étude de G. Hornung et F. Boehm préc., note 62.

²⁹⁷ Avis préc. du CEPD, 9 févr. 2012, pt 24.

présents des enjeux diplomatiques. Cette carence pose indirectement la question de l'effectivité des progrès institutionnels européens en matière de protection des libertés individuelles.

§ 1 – Une validation inattendue de l'accord par le Parlement européen

Malgré des prises de positions critiques envers l'accord PNR conclu avec les États-Unis, le Parlement européen a décidé, à travers une résolution en date du 5 mai 2010, de reporter le vote sur la demande d'approbation de cet accord PNR avec les États-Unis, faisant valoir que certaines conditions minimales devaient être remplies afin de satisfaire aux exigences européennes de protection des droits fondamentaux. Il a ainsi fait usage de sa nouvelle prérogative, issue du Traité de Lisbonne, consistant à mettre en œuvre un pouvoir d'approbation sur les accords négociés entre l'Union européenne et des États tiers, en vue de leur conclusion²⁹⁸.

Le 2 décembre 2010, le Conseil a autorisé la Commission à négocier avec les États-Unis un nouvel accord sur le transfert des données PNR qui a été paraphé le 17 novembre 2011²⁹⁹. Ce texte prévoit, d'une part, le transfert de 19 « éléments de données »³⁰⁰, notamment le nom des passagers, l'achat de leur billet et leur itinéraire de voyage.

D'autre part, ce texte transfère un ensemble de garanties, notamment en ce qui concerne la limitation de l'objectif du traitement des données à la lutte contre le terrorisme et les formes graves de criminalité transnationale, la durée de conservation des données, ainsi que le partage des données obtenues, soit à l'intérieur du pays destinataire, soit avec des pays tiers. Il évoque également la surveillance de l'accès à la base de données, y compris par le biais de l'enregistrement des transactions et des sanctions en cas d'accès non autorisé. Il interdit les décisions prises uniquement sur la base d'un traitement automatisé, tel que le refus d'accès au territoire basé uniquement sur le résultat d'une analyse informatique sans intervention humaine. En ce qui concerne les informations collectées, la question la plus délicate concerne les données sensibles, qu'il encadre. De plus, le respect de l'accord est également soumis à un contrôle conjoint, avec des évaluations sur place menées par la Commission européenne au nom de l'Union européenne.

²⁹⁸ S. PEYROU, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », Droits fondamentaux, Europe, *Revue Mensuelle LexisNexis Jurisclasseur*, juillet 2012.

²⁹⁹ Commission européenne, Proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure, COM(2011) 807 final, 23 novembre 2011.

³⁰⁰ C. FÉRAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », *Praxis CyberDroit*, Dalloz, 2020-2021.

L'adoption par la Commission d'une communication relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers a précédé l'adoption d'un cadre juridique pour l'UE dans ce domaine³⁰¹. Cette communication avait pour objectif de définir les éléments d'une démarche globale européenne vis-à-vis des données des dossiers passagers, avec, d'une part, la mise en place d'un cadre juridiquement sûr pour les transferts des dossiers passagers vers le ministère de la sécurité intérieure américain et, d'autre part, l'adoption d'une politique intérieure européenne relative aux dossiers passagers. Elle prônait également la mise au point par les transporteurs aériens d'un système de transfert de données de type « push ». Enfin, elle encouragerait la présentation d'une initiative internationale sur les transferts de données PNR par l'Organisation de l'aviation civile internationale (OACI).

Le Parlement européen, quant à lui, a rappelé dans une résolution du 11 novembre 2010 que l'objectif, s'agissant des accords PNR, était de faire en sorte que « le transfert de données soit conforme aux normes européennes en matière de protection des données »³⁰². Il a par ailleurs souligné le rôle clé joué ici par le principe de proportionnalité et est allé jusqu'à s'interroger sur la pertinence même de la collecte, du stockage et du traitement des données PNR pour les objectifs énoncés. Le Parlement européen a au même titre invité la Commission à « envisager d'autres solutions moins importunes », moins « intrusives » comme cela sera rappelé après le G29³⁰³. Le Parlement européen a toujours exprimé une préoccupation constante pour la protection des droits fondamentaux, en particulier en ce qui concerne la sauvegarde des données personnelles. Cette préoccupation est soulignée par son inscription "constitutionnelle" dans l'article 8 de la Charte des droits fondamentaux de l'Union européenne, qui est désormais juridiquement contraignante et sujette à une action en justice.

Dans le droit fil de cet article, la Commission, dans sa communication relative à la stratégie pour la mise en œuvre effective de la Charte des droits fondamentaux de l'UE, a affirmé que « l'action de l'Union doit être irréprochable en matière de droits fondamentaux ». Elle a également souligné « l'obligation de respecter les droits fondamentaux également dans les activités extérieures de l'Union »³⁰⁴. Cette affirmation se trouve dans le document de travail des orientations opérationnelles sur la prise en compte des droits fondamentaux dans les

³⁰¹ Groupe « Article 29 », Avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, adopté le 12 novembre 2010, WP 178. V. le II, p. 3.

³⁰² Commission européenne, Communication de la Commission du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, COM(2010)492 final, 21 sept 2010.

³⁰³ Ibidem

³⁰⁴ O. DE SCHUTTER, « Les droits fondamentaux dans l'Union européenne », *Journal de droit européen*, 2012, p. 114.

analyses d'impact de la Commission³⁰⁵. Or, l'approbation par le Parlement européen semble pour le moins en contradiction avec ces précédentes prises de position.

Le nouvel accord PNR de 2012 conclu entre les États-Unis et la Commission européenne, après une année de négociations, a été entériné par une décision du Conseil le 8 décembre 2011. Fortement critiqué³⁰⁶, l'accord a dû franchir les fourches caudines du Parlement européen. Compte tenu des multiples griefs à l'égard du texte initial, son approbation semblait difficile. D'ailleurs, le rapporteur du texte, vice-présidente de la commission des libertés civiles au Parlement européen, a prôné le « non » au moment du vote après avoir publiquement critiqué le texte et exprimé son désaccord publiquement, le jugeant contraire à la législation européenne et ne répondant pas aux standards énoncés par le Parlement³⁰⁷.

Cependant, de manière surprenante, la Commission des libertés civiles du Parlement européen a validé le texte dans une recommandation en date du 3 avril 2012³⁰⁸, certes assortie d'une opinion minoritaire très critique estimant que l'accord « n'apport[ait] pas les garanties exigées par le Parlement européen dans ses précédentes résolutions, (...) ces garanties [étant] de véritables lignes rouges »³⁰⁹. Finalement, le 19 avril 2012, le Parlement européen a adopté, en séance plénière, le texte de l'accord par 409 voix pour, 226 voix contre, et 33 abstentions.

Une députée hollandaise, fermement hostile à l'adoption du texte négocié, a retiré son nom du rapport, se dissociant ainsi publiquement de cet accord. Le Conseil a adopté la décision de conclusion de l'accord PNR le 26 avril 2012. L'accord est entré en vigueur le 1^{er} juin 2012. Sans surprises, les députés ont rejeté une proposition de soumettre l'accord à la Cour de justice européenne.

§ 2 – Un revirement de la position contestataire du Parlement européen vis-à-vis de l'accord PNR

Depuis l'arrêt d'annulation de la décision d'adéquation adoptée par la Commission au mépris des pouvoirs lui étant attribués par la directive 95/46, le Parlement européen est devenu l'acteur principal de la contestation de l'accord PNR signé avec les États-Unis. En effet, la

³⁰⁵ Commission, SEC(2011), 567 final, 6 mai 2011.

³⁰⁶ S. PEYROU, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », Droits fondamentaux, Europe, *Revue Mensuelle LexisNexis Jurisclasseur*, juillet 2012.

³⁰⁷ Ibidem

³⁰⁸ Voir : recommandation A7-009/2012, 3 avril 2012. Le texte a été adopté par 31 voix pour, 23 contre et 1 abstention.

³⁰⁹ Opinion minoritaire de Jan Philipp Albrecht et Rui Tavares qui ont ainsi noté que « la Commission n'a pas présenté d'éléments factuels à l'appui de son affirmation selon laquelle le stockage et le traitement des données des passagers à des fins répressives sont nécessaires et proportionnées et elle n'a jamais étudié sérieusement d'autres solutions portant moins atteinte à la vie privée ».

CJUE, saisie par les eurodéputés, majoritairement libéraux, a décidé, le 30 mai 2006³¹⁰, d'annuler l'accord de Washington du 28 mai 2004 au motif que la décision d'adéquation prise par la Commission ne relevait pas du champ d'application de la directive 95/46 sur laquelle elle a fondé sa décision.

La directive 95/46 exclut effectivement de son champ d'application le traitement des données « ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal »³¹¹. Or, les juges ont raison de rappeler que le transfert des données PNR « constitue un traitement ayant pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal »³¹². Par ailleurs, pour des raisons de sécurité juridique, la Cour a prévu que les effets de la décision d'adéquation de la Commission seraient toutefois maintenus jusqu'au 30 septembre 2006.

L'annulation revêtait une importance symbolique, car la décision d'adéquation marquait le début de l'implication de la Communauté européenne dans la lutte contre le terrorisme menée par les États-Unis. Cependant, il est essentiel de souligner que la décision d'adéquation est principalement et avant tout une mesure d'exécution de la directive 95/46. C'est justement cette double dimension qui est au cœur de la remise en cause de la légalité de l'acte adopté par la Commission³¹³. Les exigences de la hiérarchie des normes imposent à la Commission, en tant qu'organe exécutant un acte de droit dérivé, de se conformer à celui-ci. Or, l'article 3 § 2 prévoit l'exclusion des traitements de données qui sont « mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles celles prévues au titre V et VI du Traité UE, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal »³¹⁴. La qualification de la finalité du traitement des données des passagers aériens a fait l'objet d'un débat devant la CJUE.

La réfutation de l'accord PNR ayant pour objet la sécurité publique a été débattue. En effet, c'est bien en raison du transport de passagers en direction des États-Unis³¹⁵ que des transferts

³¹⁰ CJCE 30 mai 2006, aff. C-317/04 et C-318/04, Parlement européen c/ Conseil de l'Union européenne et Commission des Communautés européennes, Rec. I-04721s.

³¹¹ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

³¹² CJCE 30 mai 2006, aff. C-317/04 et C-318/04, Parlement européen c/ Conseil de l'Union européenne et Commission des Communautés européennes, Rec. I-04721s.

³¹³ A. VAUCHEZ, *L'union par le droit, L'invention d'un programme institutionnel pour l'Europe*, Presses de Science Po, 2013.

³¹⁴ Directive EU 95/46, Article 3 § 2.

³¹⁵ Technologie et souveraineté, « Entretien avec Régis Debray, Propos recueillis par Olivier de France, François-Bernard Huyghe, Marc Verzeroli », *Revue internationale et stratégique*, n° 110, 2018, pp. 51-59. Pour

de données sont requis, ainsi l'origine des transferts n'est autre qu'une obligation mise à la charge des compagnies aériennes dans l'exercice de leurs activités économiques. D'ailleurs, la Cour a considéré que « les données PNR sont initialement collectées par les compagnies aériennes dans le cadre d'une activité qui relève du droit communautaire » et donc, en l'espèce, d'une prestation de service³¹⁶. Les activités des compagnies aériennes sont donc celles de personnes privées.

Toutefois, cet aspect ne peut être appréhendé isolément. Plus précisément, il ne s'agit là que d'une première étape dans le processus d'utilisation des données PNR, à savoir la collecte de données. Or, il est indubitablement inexact de ne considérer que ce seul élément car les données de passagers collectées le sont surtout à une fin déterminée. L'utilisation de ces données par le ministère de l'Intérieur américain, notamment le CBS (autorité en charge des frontières), dans le cadre de l'exercice d'une fonction sécuritaire, correspond à la mise en œuvre d'une législation américaine dont l'objectif est de renforcer la sécurité afin de prévenir le terrorisme.

La Commission elle-même confirme bien que « les données PNR doivent être utilisées dans le but unique de prévenir et de combattre le terrorisme et les crimes liés au terrorisme »³¹⁷. Par conséquent, la finalité du transfert des données des passagers aériens, comme les conditions d'intervention de leur destinataire, sont formellement étrangères à la sphère économique³¹⁸.

§ 3 - Un reversement du Parlement européen aux visées diplomatiques

L'accord PNR a révélé un problème existentiel qui se pose à l'Union européenne depuis les origines. En effet, un constat amer s'impose : le droit peut difficilement peser face aux enjeux diplomatiques. Partant, se pose indirectement la question de l'effectivité des progrès institutionnels réalisés par le Traité de Lisbonne. De fait, un certain nombre de considérations politiques semblent avoir pesé sur le vote des parlementaires, ce qui explique que si le Parlement européen a émis des réserves dans son avis publié le 9 décembre 2011, il n'a pas

Régis Debray « ce sont les États-Unis qui standardisent nos gestes quotidiens et fixent nos normes de conduite. Ils fournissent le mode d'emploi avec les appareils, plus encore dans le numérique ». L'auteur a pu développer cette idée dans son ouvrage *Civilisation* (Gallimard, 2017) en considérant que l'hégémonie américaine couvre notamment l'Europe, notamment du point de vue de la norme juridique.

³¹⁶ V. MICHEL, « La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration », *Revue trimestrielle de droit européen*, Dalloz, 2006.

³¹⁷ Décis. 2004/535 de la Commission, du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au bureau de douanes et de la protection des frontières des États-Unis d'Amérique, JOUE L 235, 6 juill. 2004, p. 11.

³¹⁸ V. MICHEL, « La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration », *Revue trimestrielle de droit européen*, Dalloz, 2006.

pour autant fait usage du droit de veto dont il dispose sur ce type d'accords en vertu du Traité de Lisbonne³¹⁹.

D'abord, des menaces à peine voilées de la part des États-Unis semblent avoir été émises et ces derniers paraissaient être prêts à revenir sur leur décision d'exemption de visas octroyée aux citoyens de la plupart des pays de l'Union européenne pour voyager sur leur territoire³²⁰. Ensuite, il a semblé aux parlementaires que le refus de signer l'accord n'était pas nécessairement préférable, car en l'absence d'accord, et donc de base juridique commune pour le transfert aux États-Unis des données des passagers aériens européens, les transporteurs aériens, soumis un moment ou un autre au droit américain se seraient retrouvés face à un vide juridique, ce qui n'est naturellement pas enviable³²¹. Par ailleurs, les États-Unis disposent toujours la voie bilatérale pour conclure, au cas par cas, des accords avec les pays concernés, fragilisant ainsi la position de l'Union européenne. Cette dernière voie n'est clairement pas plus avantageuse pour la protection des droits fondamentaux des Européens.

Ainsi, la députée hollandaise qui a fortement critiqué l'accord, à laquelle il a été précédemment fait référence, s'est demandé si « on peut accepter tout et n'importe quoi »³²², remettant ainsi en cause un certain réalisme politique au centre de la sauvegarde de la bonne coopération transatlantique, notamment en matière de lutte contre le terrorisme. La diplomatie a donc pris le dessus sur les droits fondamentaux. Du reste, la décision validant l'accord, critiquable dans la mesure où ce dernier ne respecte manifestement pas « la vie privée des citoyens européens et [est] contraire aux lois et principes sur la protection des données » aux dires aussi bien du CEPD ou du G29 que du Parlement européen lui-même, présente un autre risque, non moins préoccupant pour le droit européen. En effet, un certain nombre d'autres États, comme l'Arabie Saoudite, les Émirats Arabes Unis, la Russie et la Corée du Sud, ont affiché leur intérêt pour une coopération sur les données PNR. Le soutien de ces États pousse à se poser la question de savoir si cet accord n'a pas ouvert la voie à un précédent dangereux pour les droits fondamentaux des Européens.

D'autres parlementaires ont insisté sur l'objectif sécuritaire de l'accord : « nous avons fait en sorte que cet accord soit uniquement utilisé pour prévenir, détecter et poursuivre devant la justice les graves crimes transnationaux et le terrorisme » ; tout en rappelant la préoccupation

³¹⁹ L. GRARD, « Chronique Droit européen des transports - Sécurité aérienne : nouveaux accords internationaux sur le transfert des données personnelles des passagers », *Revue trimestrielle de droit européen*, Dalloz, 2013.

³²⁰ S. PEYROU, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », *Droits fondamentaux, Europe, Revue Mensuelle LexisNexis Jurisclasseur*, juillet 2012.

³²¹ Ibidem

³²² S. IN'T VELD, *Europolitique*, 20 avr. 2012, n° 4409.

des droits fondamentaux puisque « les passagers verront leurs données protégées. Ils bénéficieront d'un droit d'accès et de correction, ainsi que d'une possibilité de savoir comment leurs informations pourraient être utilisées. Les données sensibles, tel que le choix des repas, seront utilisées dans des circonstances très exceptionnelles et dépersonnalisées après six mois »³²³.

L'accord a naturellement été reçu positivement par le représentant américain auprès de l'Union européenne, confirmant l'influence diplomatique américaine sur cette législation européenne. Ce dernier a pu considérer que ce transfert des données « a aidé dans pratiquement toutes les enquêtes américaines de premier plan sur le terrorisme au cours des dernières années » pour freiner le terrorisme aérien³²⁴.

Quant à la commissaire européenne chargée du dossier, elle a reconnu que l'accord n'était « pas parfait à 100% » mais a assuré que le texte respectait « pleinement le droit européen »³²⁵. Cette dernière a d'ailleurs repris l'argument suivant : en cas de rejet du texte négocié, les données auraient continué à être collectées par les autorités américaines mais hors de tout cadre juridique, limitant ainsi les possibilités pour les citoyens européens de contrôler l'utilisation de leurs données personnelles de passagers aériens.

§ 4 – Un Parlement européen mis sous pression par la Commission européenne dans le cadre de la lutte contre le terrorisme

Cette séquence a marqué un déséquilibre au sein de l'Union européenne entre la nécessité de protection des libertés et l'impératif de sécurité ; entre la protection des données à caractère personnel et la lutte contre le terrorisme³²⁶. L'absence de veto du Parlement européen indique que les objectifs de rééquilibrage entre sécurité et liberté annoncés par le Programme de Stockholm ne sont pas faciles à atteindre.

Adopté par le Conseil européen de Bruxelles, les 10 et 11 décembre 2009, le Programme de Stockholm³²⁷ déterminait le cadre relatif à la coopération policière et douanière, à la coopération entre les services de sauvetage, à la coopération judiciaire en matière pénale et

³²³ Rédaction, « Transfert des données des passagers aériens : pour ou contre ? », Europa, *Actualité Parlement Européen*, 2012.

³²⁴ Rédaction Europe1 avec AFP, « Vol vers les USA : vos données voyagent aussi », *Europe 1*, 19 avril 2012.

³²⁵ Ibidem

³²⁶ P. BERTHELET, Y. EL BOUSTANI, L. FRIEL, L. ROBERT, N. PRADEL..., « Le volet externe de l'espace de liberté, de sécurité et de justice : instruments et réalisations », *Revue trimestrielle de droit européen*, Dalloz, 2014.

³²⁷ S. CARRERA, E. GUILD, Does the Stockholm Programme matter?, The struggles over ownership of AFSJ, Multiannual programming, *Liberty and security in Europe*, n° 51, 2012, en ligne à URL [http://aei.pitt.edu/38964/1/No_51_Carrera_and_Guild_on_Swedish_Programme\[1\].pdf](http://aei.pitt.edu/38964/1/No_51_Carrera_and_Guild_on_Swedish_Programme[1].pdf), consulté le 24 septembre 2023.

répressive, ainsi qu'à d'autres questions portant sur les politiques d'asile, de migration et de visas pour la période 2010 – 2014. Ce document identifiait les priorités suivantes : promotion des droits des citoyens de l'Europe, amélioration de la vie quotidienne, protection civile, accès à l'espace européen, solidarité et partenariat en matière de migrations et d'asile ainsi que la dimension extérieure de l'espace de Liberté, de Sécurité et de Justice. En ce qui concerne la dimension extérieure de la coopération en matière répressive, il est apparu, pour reprendre les termes du Conseil, que « certains objectifs du programme de Stockholm [...] ont été réalisés tandis que d'autres n'ont progressé que de manière limitée »³²⁸.

L'action du Parlement européen³²⁹ s'est inscrite dans un contexte marqué par l'intensité des relations entre l'Union européenne, l'ONU et les États-Unis dans des domaines tels que le terrorisme, la criminalité, ou encore la corruption ; domaines pour lesquels la nécessité d'une action globale a fait consensus. L'Union européenne a souhaité s'affirmer en la matière, en tant qu'acteur international, en adhérant à la logique sécuritaire transnationale censée répondre aux défis posés par l'expansion globale du champ criminel³³⁰. Cette position a rendu l'affirmation de la protection des droits fondamentaux bien timide face à l'impératif de lutte contre le terrorisme. L'absence de veto du Parlement européen témoigne de l'incapacité des dirigeants européens à infléchir la position de leurs homologues américains.

La coopération euro-américaine a été marquée ces deux dernières décennies par la conclusion de deux accords controversés concernant la collecte et l'échange d'informations aux fins de lutte contre le terrorisme. Le premier est un accord sur le transfert de données de messagerie financière de l'Union européenne vers les États-Unis aux fins du programme de surveillance du financement du terrorisme (TFTP dit « SWIFT ») en 2010³³¹. Le second est l'accord sur le transfert de données PNR conclu en 2012, après huit ans d'âpres négociations. Ces deux accords ont pour trait commun d'avoir cristallisé une lutte entre le Parlement et le Conseil.

³²⁸ Conseil de l'Union européenne, *Évaluation à mi-parcours du programme de Stockholm*, Note, Bruxelles, 13 novembre 2012, en ligne à URL : <http://www.gdr-elsj.eu/wp-content/uploads/2012/12/Doc-15921.12-Evaluation-Stockholm.pdf> consulté le 23 septembre 2023.

³²⁹ F. MASSART-PIERARD, « Le Parlement européen : l'irrésistible mouvement de conquête des pouvoirs », *Revue internationale de politique comparée*, 2009, pp. 545-557, en ligne à URL : <https://www.cairn.info/revue-internationale-de-politique-comparee-2009-4-page-545.htm> consulté le 23 septembre 2023.

³³⁰ P. BERTHELET, Y. EL BOUSTANI, L. FÉRIEL, L. ROBERT, N. PRADEL..., « Le volet externe de l'espace de liberté, de sécurité et de justice : instruments et réalisations », *Revue trimestrielle de droit européen*, Dalloz, 2014.

³³¹ Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, 2010. Lire en ce sens. A. MATTELART, « La guerre sans fin, le paradigme technosécuritaire » in *La Globalisation de la surveillance*, La Découverte, 2008, pp.166-192. L'auteur considère que la maîtrise des réseaux d'information et de communication fait partie des nouveaux piliers de la politique américaine pour la préservation de son statut de superpuissance.

Malgré divers amendements, les deux textes ont été jugés attentatoires aux standards européens de protection des droits fondamentaux³³².

Avec l'accord PNR, l'Union européenne a semblé tenir un double langage, puisque d'un côté elle affirmait soutenir des normes élevées en matière de protection des données personnelles au nom des droits de l'Homme, et de l'autre, elle accepta le transfert des données des citoyens européens aux États-Unis, sans refuser l'imposition de normes américaines incompatibles avec ses standards. Ces compromissions de l'Union européenne sont des « violations[s] consentie[s] au nom du réalisme politique »³³³ et sous pressions diplomatiques importantes. En plus de constituer un dangereux précédent de l'Union européenne à l'égard des pays tiers, ces compromissions peuvent être synonyme de nivellement vers le bas en matière de protection des données personnelles.

L'accord PNR entre les États-Unis et l'Union européenne montre que la Commission, organe responsable de la conduite des négociations dont le mandat est défini par le Conseil, n'a pas été « en mesure d'imposer avec fermeté la défense du modèle européen »³³⁴, révélant ainsi la transposition de la réalité des rapports de force politique dans le monde qui s'est manifestée dans la négociation déséquilibrée entre deux grands acteurs internationaux. Une lecture politique de cet acte juridique peut potentiellement être traduite comme l'incursion d'une autorité étrangère dans la souveraineté des États européens à travers un système d'extraction de données. Or, en application des règles du droit international, les États concernés doivent y consentir, par la signature formelle d'accords internationaux conclus avec l'autorité américaine. Par ailleurs, à considérer que cet accord crée un précédent, il paraît inconcevable qu'une telle « incursion » soit envisageable par le biais d'un accord avec la Chine ou la Russie.

§ 5 – Les données des passagers aériens au centre de la complexité institutionnelle de l'Union européenne

La montée en puissance du traitement des données dans le champ sécuritaire a nourri les débats sur le rôle de chaque institution au sein de l'Union européenne. Les données sont au centre de la réponse sécuritaire que l'Union entend apporter à ses citoyens. Utilisées aussi bien dans le cadre des politiques migratoires que celui de la coopération policière et judiciaire du

³³² P. BERTHELET, Y. EL BOUSTANI, L. FRIEL, L. ROBERT, N. PRADEL..., « Le volet externe de l'espace de liberté, de sécurité et de justice : instruments et réalisations », *Revue trimestrielle de droit européen*, Dalloz, 2014.

³³³ F. MARIATTE, « Protection des données personnelles des usagers des transports aériens », *Nouvelles technologies*, Europe n° 7, juillet 2004.

³³⁴ V. MICHEL, « La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration », *Revue trimestrielle de droit européen*, 2006.

troisième pilier, ces données personnelles concernent le système Schengen et les visas mais également l'entraide policière d'Europol³³⁵.

En effet, la mise en œuvre du marché unique qui s'est accompagnée de la suppression des contrôles aux frontières intérieures a entraîné des conséquences liées à la libre circulation des personnes. L'Union européenne souhaite éviter que ce grand espace européen n'encourage des trafics illégaux d'un pays à l'autre ou en provenance de pays tiers. Les dispositions législatives et réglementaires nationales des États membres, dans leur diversité, devaient se coordonner dans les domaines de l'immigration, de lutte contre le terrorisme, de trafic de drogue, d'armes et d'œuvres d'art et en matière de criminalité organisée. Lors des négociations du Traité de Maastricht, le chancelier allemand Kohl a insisté sur la nécessité de mieux contrôler les mouvements de population en citant l'exemple de son pays, l'Allemagne, qui a accueilli de nombreux immigrants d'Europe de l'Est³³⁶.

Le traité sur l'Union européenne a aspiré à répondre à ces préoccupations avec la mise en place d'un troisième pilier intitulé « Justice et Affaires intérieures » (JAI)³³⁷, à la suite d'un premier pilier « Communauté européenne » (CE) et le deuxième « Politique étrangère et de sécurité commune » (PESC). Des domaines d'intérêts communs ont été énumérés : politique d'asile, lutte contre la toxicomanie et la fraude de dimension internationale, règles régissant le franchissement des frontières extérieures de l'Union, politique à l'égard des ressortissants des pays tiers et politique d'immigration, coopération judiciaire en matière civile et pénale, coopération douanière et policière. Cette reconfiguration n'enlève pas aux États leurs prérogatives régaliennes : ils conservent les responsabilités de la sauvegarde de la sécurité intérieure et du maintien de l'ordre public³³⁸.

S'agissant des matières très sensibles relevant de la souveraineté, c'est la méthode intergouvernementale qui est employée. La Commission européenne ne dispose pas du monopole de proposition mais se trouve concrètement associée aux travaux. Par ailleurs, les États membres peuvent également faire des propositions. D'ailleurs, ils sont les seuls à pouvoir le faire dans les domaines sensibles, notamment ceux de la coopération douanière et policière, et la coopération judiciaire pénale. Dans le cadre de ce système, le Conseil des

³³⁵ H. LABAYLE, « Architecte ou spectatrice ? La Cour de justice de l'Union dans l'Espace de liberté, sécurité et justice », *Revue trimestrielle de droit européen*, 2006, p. 1.

³³⁶ The Centre Virtuel de la Connaissance sur l'Europe, « Le troisième pilier de l'Union européenne : justice et affaires intérieures ».

³³⁷ A. BIAVA, « L'Union européenne, acteur global ? Potentialités et limites de la PESC et de la PESD », *Europa*, Institut européen de l'Université de Genève, 2005.

³³⁸ A. MÉGIE, « Généalogie du champ de la coopération judiciaire européenne », in *Arrêter et juger en Europe, Cultures & Conflits*, L'Harmattan, n° 62, 2006.

ministres adopte à l'unanimité des positions partagées et peut décider des actions communes. Des mesures d'application pourront être prises à la majorité qualifiée si ce dernier en décide, ainsi qu'à l'unanimité. Toutefois, à la différence des règlements et directives européennes, ces actions communes n'obligent les gouvernements qu'à les soumettre à leur parlement qui est libre de les adopter ou non.

Des rapports sont prévus entre les deux piliers du fait de l'imbrication des compétences du pilier JAI avec celles de la Communauté relatives au marché unique et à la libre circulation. Par exemple, pour les visas, une politique commune est nécessaire pour des raisons d'efficacité afin d'éviter qu'un afflux d'immigrants naisse dans un pays à la politique migratoire laxiste et se répande ensuite librement chez ses voisins. Aussi, la politique des visas a été confiée à l'Union européenne, les décisions étant préparées par la Commission à la demande d'un État membre. En effet, l'exigence d'unanimité risque d'aboutir à l'impossibilité d'élaborer une politique commune. D'autre part, le Comité de coordination chargé de préparer les travaux du Conseil doit assurer ces fonctions aussi bien pour les matières relevant de la compétence communautaire que pour celles du pilier JAI.

Enfin, le traité a prévu une « passerelle » permettant de transférer au pilier communautaire, dans un souci d'efficacité, des matières relevant du pilier JAI, à l'exception de la coopération policière, de la coopération judiciaire pénale et de la coopération douanière. Il en a été décidé ainsi par le traité d'Amsterdam du 2 octobre 1997.

Lorsqu'elle a conclu en 2004 l'accord controversé avec les États-Unis concernant le transfert des données à caractère personnel³³⁹, l'Union européenne s'est basée sur l'article 95 TCE relatif « au rapprochement des dispositions législatives, réglementaires et administratives des États membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur »³⁴⁰. Cet accord s'est naturellement inscrit dans le respect de la directive 95/46 et s'appuyait en ce sens sur une « décision d'adéquation » de la Commission. Or, faute de pouvoir pour le réformer, le Parlement l'a contesté par la voie contentieuse tout comme la décision du Conseil de conclure un tel accord, sans s'appuyer sur la base juridique fournie par l'article 300 § 3 TCE, qui implique un avis conforme du Parlement européen.

³³⁹ Procès-verbal de rectification de l'accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure (JO L 183 du 20.5.2004).

³⁴⁰ Traité instituant la Communauté européenne, Nice, 1995.

Constatant ces prétentions contradictoires, l'avocat général Philippe Léger³⁴¹ a mis au grand jour la complexité institutionnelle de l'action européenne en matière de traitement des données dans le champ sécuritaire. En effet, le conflit de bases juridiques se situe plus entre les deux piliers communautaire et intergouvernemental qu'à l'intérieur du Traité communautaire.

L'accord PNR était mis en avant au motif qu'il devait urgemment servir les finalités de la réalisation du marché intérieur et éviter des distorsions de concurrence entre les compagnies aériennes européennes et leurs homologues américains. Mais cet argument du Conseil paraît secondaire par rapport à son objectif principal, puisque le paragraphe premier du préambule de l'accord indique « qu'il importe de respecter les droits et libertés fondamentaux, et notamment le droit au respect de la vie privée, et de respecter ces valeurs, tout en prévenant et en combattant le terrorisme et les délits qui y sont liés, ainsi que d'autres délits graves de nature transnationale, notamment la criminalité organisée »³⁴². Or, ces préoccupations sont difficiles à relier à un titre de compétence communautaire.

D'ailleurs, la décision d'adéquation de la Commission a posé un problème de compétence, car elle se réclame de la directive 95/46 dont le champ d'application est limité : « ... la présente directive ne s'applique pas au traitement de données à caractère personnel ... mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du Traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal »³⁴³.

Les fondements communautaires de la démarche de coopération répressive avec les États-Unis ne sont pas solides et les conclusions de l'avocat général l'ont exprimé, sans détours, dès lors que cette « affaire concerne en réalité une problématique nouvelle, qui est relative à l'utilisation de données commerciales à des fins répressives »³⁴⁴. Manifestement, la décision d'adéquation est vue comme nécessaire pour la sauvegarde de la sécurité publique et à des fins répressives. Par conséquent, elle ne vise pas un traitement de données nécessaire à la réalisation d'une prestation de services³⁴⁵. Autorisant à transmettre des données à un État tiers

³⁴¹ Conclusions sur l'affaire Parlement c/ Conseil, C-317/04, présentées le 22 novembre 2005.

³⁴² Ibidem

³⁴³ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

³⁴⁴ H. LABAYLE, « Architecte ou spectatrice ? La Cour de justice de l'Union dans l'Espace de liberté, sécurité et justice », *Revue trimestrielle de droit européen*, 2006, p. 1.

³⁴⁵ Ibidem

afin de lutter contre le terrorisme, l'accord passé avec les États-Unis « tente de concilier deux objectifs, c'est-à-dire qu'il repose sur l'idée selon laquelle la lutte contre le terrorisme et d'autres crimes graves doit être menée dans le respect des droits fondamentaux, notamment du droit au respect de la vie privée, et plus précisément du droit à la protection des données à caractère personnel »³⁴⁶. Cette erreur de base juridique, démontrée par l'avocat général, aurait dû alerter les autorités européennes sur les risques de l'annulation, qui n'a pas tardé à venir des années plus tard.

La contestation de la base juridique a ouvert la voie à des décisions qui vont tenter de sanctuariser l'organisation des compétences distribuées par le Traité sur l'Union dans sa partie intergouvernementale. Par ailleurs, cette situation a nourri une crainte : l'annulation contentieuse domine désormais l'ensemble des débats qui entourent les législations relatives au droit de l'espace de sécurité, de liberté et de justice (ESLJ)³⁴⁷. Ainsi, dans le cas des données PNR, l'objectif de sécurité juridique se recoupe avec des arrière-pensées politiques. Or, face à l'impossibilité de réunir l'unanimité au Conseil, la conséquence directe qui découle de cette situation est celle de contraindre l'Union européenne à sacrifier la qualité du texte en discussion. La codécision, comme la majorité qualifiée, ouvrent des opportunités de contournement et des marges de négociation que le veto à l'unanimité écarte d'emblée.

³⁴⁶ Ibid.

³⁴⁷ Ibid.

Chapitre 2 – Le consensus des législations répressives sur la finalité sécuritaire des dossiers passagers

Les deux dernières décennies ont vu une éclosion des mesures de lutte de contre le terrorisme³⁴⁸, aussi bien sur le plan international et qu'à l'échelle nationale. La résolution 1624 (2005) du Conseil de sécurité, adoptée le 14 septembre 2005, a demandé au Comité contre le terrorisme d'assister les États membres dans la prévention de l'incitation à commettre des actes terroristes. En effet, le Conseil avait appelé les États membres à « introduire des législations répressives pour interdire, par la loi, l'incitation à commettre un ou des actes terroristes, prévenir une telle incitation et refuser l'asile à toute personne au sujet de laquelle on dispose d'informations crédibles et pertinentes selon lesquelles il existe des raisons sérieuses de penser qu'elle est coupable d'une telle incitation »³⁴⁹.

À travers des sanctions pénales et administratives, ces législations répressives, définies par Yves Mayaud, se distinguent par des qualifications autonomes et l'existence de peines originales³⁵⁰. En France, l'article 421-3 du code pénal a ainsi prévu le maximum de la peine privative de liberté pour les infractions terroristes. Le maximum de la peine privative de liberté encourue pour les infractions mentionnées à l'article 421-1 du code pénal est relevé d'un degré par rapport à l'infraction d'origine : à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle ; trente ans lorsque l'infraction est punie de vingt ans ; vingt ans lorsque l'infraction est punie de quinze ans ; quinze ans lorsque l'infraction est punie de dix ans ; dix ans lorsque l'infraction est punie de sept ans ; sept ans lorsque l'infraction est punie de cinq ans. L'emprisonnement est porté au double lorsque l'infraction est punie de trois ans au plus, selon l'article 421-3 du code pénal. Pour ce qui est des autres peines principales encourues, elles sont considérées comme étant identiques.

³⁴⁸ La formule de « guerre contre le terrorisme » a été employée par l'administration américaine après les attentats du 11 septembre 2001 mais elle a été critiquée en France et ailleurs dans le monde pour son caractère « divisive ». Voir C. BERTRAM, « Notre guerre contre le terrorisme », in *Justifier la guerre*, Presses de Science Po, 2013, pp. 221-238. Voir aussi. C. EMANUELLI, Faut-il parler d'une "guerre" contre le terrorisme? *Canadian Yearbook of international Law/Annuaire canadien de droit international*, 2009 ; D. WILLS, *The First War on Terrorism: Counter Terrorism during the Reagan Administration*, Lanham, Rowman and Littlefield, 2003 ; F. MÉGRET, "“War”? Legal Semantics and the Move to Violence," *European Journal of International Law*, 2002, p. 361.

³⁴⁹ Résolution 1624, Conseil de sécurité, ONU, 2005.

³⁵⁰ Y. MAYAUD, « Terrorisme – Infractions », *Répertoire de droit pénal et de procédure pénal*, Dalloz, janvier 2022.

Les législations contre le terrorisme sont donc dites répressives puisque de nombreuses infractions du code pénal servent de support à son incrimination³⁵¹. En France, le droit pénal ne se limite pas à criminaliser uniquement les actes de terrorisme ; il sanctionne également les comportements qu'il considère comme relevant de sa politique d'incrimination. Le code pénal prend le parti de l'innovation « en opérant une distinction entre deux types de terrorisme : le terrorisme dérivé dont le principe procède d'un adossement à des infractions existantes, et le terrorisme qualifié relevant quant à lui d'une conception plus autonome »³⁵². Ainsi, les actes de terrorisme sanctionnés en France sont regroupés dans le code pénal au sein des crimes et délits contre la Nation, l'État et la paix publique. Ces infractions ont toutes en commun d'être commises intentionnellement et en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur³⁵³.

Pionnier, le droit américain est le premier à avoir initié l'utilisation des dossiers passagers (données personnelles des passagers aériens) afin de lutter contre le terrorisme³⁵⁴ et le crime organisé, après une série d'attaques visant les aéronefs sur le sol américain. L'accord³⁵⁵ entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, en date du 11 août 2012, est venu parachever une évolution de l'usage sécuritaire des dossiers passagers, confirmant ainsi une vision commune entre Américains et Européens quant à la finalité de cette utilisation (section 1).

La directive du 27 avril 2016 relative à la prévention et la détection des infractions terroristes et formes graves de criminalité confirme l'influence américaine sur le droit européen qui a adopté une logique répressive s'agissant de l'utilisation des données personnelles des passagers aériens, le transfert des données passagers par les transporteurs aériens et leur traitement (section 2). Cette directive a cependant été précédée de plusieurs événements montrant des divergences de conception entre Américains et Européens quant aux standards de protection des dossiers passagers. Cette directive reprend également l'appel énoncé par le

³⁵¹ T.S. RENOUX, « Juger le terrorisme ? », *Cahiers du Conseil constitutionnel*, n° 14, Dossier : La Justice dans la Constitution, mai 2003, en ligne à URL : <https://www.conseil-constitutionnel.fr/node/2915/pdf> consulté le 3 octobre 2023.

³⁵² Ibidem

³⁵³ Definition in Terrorism, *Fiche d'orientation*, Dalloz, 2021.

³⁵⁴ M. H. HOFFMAN, "Rescuing the Law of War: A Way Forward in an Era of Global Terrorism", *The US Army War College Quarterly: Parameters*, Volume 35, Number 2, 2005, en ligne à URL <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2260&context=parameters> consulté le 3 octobre 2023.

³⁵⁵ House of Lords, *The EU/US Passenger Name Record (PNR) Agreement*, European Union Committee, 5 juin 2007, en ligne à URL : <https://publications.parliament.uk/pa/ld200607/ldselect/lducom/108/108.pdf> consulté le 3 octobre 2023.

Conseil de sécurité dans la résolution 1624, paragraphe 2, à savoir « coopérer, notamment en vue de renforcer la sécurité de leurs frontières internationales, en particulier en luttant contre la falsification des documents de voyage, et, dans la mesure du possible, en améliorant la détection des terroristes et les formalités visant à assurer la sécurité des passagers, en vue d'empêcher les auteurs des agissements mentionnés à l'alinéa a) du paragraphe 1 d'entrer sur leur territoire »³⁵⁶. La directive confirme la volonté des dirigeants européens de réglementer le transfert, par les compagnies aériennes, des données des dossiers passagers aux autorités nationales, ainsi que le traitement de ces données³⁵⁷.

Ces règles de l'Union européenne³⁵⁸ ont vocation à lutter contre les activités criminelles et les infractions terroristes³⁵⁹ impliquant des déplacements internationaux par avion. Ce système européen harmonise³⁶⁰ les dispositions juridiques des États membres. Par ailleurs, il vise à éviter l'insécurité juridique et les failles en matière de sécurité tout en garantissant la protection des données des passagers aériens³⁶¹.

Section 1 – Un consensus illustré par l'existence d'un accord euro-américain sur le transfert des dossiers passagers

Historiquement, les États-Unis ont soutenu la fondation de la Communauté européenne du charbon et de l'acier (CECA), reconnaissant ainsi les principes de l'intégration européenne qui s'inspirent des principes politiques et économiques présents de l'autre côté de l'Atlantique. Entre 1948 et 1952, le plan Marshall, visant la reconstruction de l'Europe, a permis le transfert depuis l'Amérique vers seize pays européens (hors bloc soviétique) d'un montant d'une valeur de près de 10% du PIB (produit intérieur brut) de ces derniers. Ce plan a joué un rôle primordial dans la croissance européenne d'après-guerre en permettant notamment de résoudre les problèmes d'approvisionnement, une libéralisation des échanges

³⁵⁶ Résolution 1624, Conseil de Sécurité, ONU, 2005.

³⁵⁷ M. BENLOLO-CARABOT, « Chronique Droit pénal de l'Union européenne – Protection des données personnelles, lutte contre le terrorisme : la CJUE confrontée à la surveillance de masse », *La Revue trimestrielle de droit européen*, Dalloz, RTD eur., 2017, p. 887.

³⁵⁸ R. TINIERE, « L'influence croissante de la Charte des droits fondamentaux sur la politique extérieure de l'Union européenne », *Revue des droits et libertés fondamentaux*, RDLF, 2018.

³⁵⁹ A. SCHERRER, A. MEGIE ET V. MITSILEGAS, « La stratégie de l'Union européenne contre la criminalité organisée : entre lacunes et inquiétudes », *Cultures & Conflits* [En ligne], 74, été 2009, 28 octobre 2010, en ligne à URL : <http://journals.openedition.org/conflits/17442> consulté le 3 octobre 2023.

³⁶⁰ Sur les difficultés d'harmonisation que cela pourrait poser, voir E. CARPANELLI et N. LAZZERINI, « PNR : Passenger Name Record, Problems Not Resolved ? The EU PNR Conundrum After Opinion 1/15 of the CJEU », *Air and Space Law*, vol. 42, Issue 4/5, 2017, pp. 377-402.

³⁶¹ N. LE BONNIEC, « L'Union européenne à l'ère du numérique et la lutte contre le terrorisme : la sécurité au détriment de l'État de droit avec les accords PNR ? », in « Quel État de droit dans une Europe en crise ? », *Chronique*, n° 44, *Revue des droits et libertés fondamentaux*, RDLF, 2019, en ligne à URL : <https://revuedlf.com/droit-ue/lunion-europeenne-a-lere-du-numerique-et-la-lutte-contre-le-terrorisme-la-securite-au-detrimet-de-letat-de-droit-avec-les-accords-pnr/> consulté le 3 octobre 2023.

intra-européens, une augmentation de la productivité grâce à l'aide technique américaine ainsi que la création d'un environnement favorable à la stabilisation et aux réformes dans les États bénéficiaires. La productivité du travail et le niveau d'investissement élevé qu'il encouragea a donné lieu à la forte croissance caractéristique de la période dite des Trente Glorieuses³⁶².

La reconnaissance de l'Europe par le gouvernement américain comme un homologue politique, notamment en matière de politique étrangère et de sécurité, n'est pas si lointaine. Ce n'est qu'au sommet euro-américain de Vienne en juin 2006 que le Président américain George H. W. Bush a mis en avant le travail en commun entre les États-Unis d'Amérique et l'Union européenne sur les grands sujets mondiaux, incluant le terrorisme international, l'immigration, la transmission mondiale des maladies, le réchauffement planétaire, l'ascension de la Chine, ou encore la violence et l'instabilité au Moyen-Orient³⁶³. Leur convergence sur ces sujets n'effaça cependant pas les divergences entre Américains et Européens quant à leur approche de la crise du réchauffement climatique, leur perception de la place des droits de l'Homme dans le corpus juridique national ou bien à propos de la détention de prisonniers, à Guantanamo ou ailleurs.

À la suite des attentats du 11 septembre 2001, les responsables européens ont très vite exprimé leur solidarité déclarant que « la lutte contre le terrorisme sera, plus que jamais, une priorité de l'UE »³⁶⁴. Les attaques terroristes à Madrid et à Londres n'ont fait que consolider cette volonté de coopération afin de lutter contre le terrorisme international. Le premier accord sur les dossiers passagers entre les États-Unis d'Amérique et l'Union européenne s'inscrivait dans un cadre plus large d'une coopération euro-américaine contre le terrorisme³⁶⁵, sous les auspices d'une stratégie et d'une vision communes contre les infractions terroristes.

La législation américaine sur l'utilisation sécuritaire des données personnelles des passagers, qui a suivi ces attentats, est venue cristalliser un mouvement commencé quelques années auparavant faisant des dossiers passagers un outil pour lutter contre les crimes qui touchent le secteur aérien (sous-section 1)³⁶⁶. Cette influence américaine n'a fait que se renforcer après les attentats terroristes du 11 septembre 2001 offrant aux promoteurs de l'usage sécuritaire

³⁶² J-B. GOSSÉ, A. SCHNEIDER, R. VICQUÉRY, « Les leçons du plan Marshall pour le plan de relance européen », *Bloc-notes Eco*, Banque de France, 29 octobre 2021.

³⁶³ J. BRUTON, « La relation euro-américain en transition », *Politique américaine*, 2006/3, n° 6, p. 15 à 24, L'Harmattan, 2006.

³⁶⁴ Ibidem

³⁶⁵ L. IDOT, « Vers une Union de la sécurité », *Europe*, n° 11, novembre 2017, alerte 57.

³⁶⁶ C. DOCKSEY, « Opinion 1/15: Privacy and security, finding the balance », *Maastricht Journal of European and Comparative Law*, vol. 24, n° 6, 2017, pp. 768-773.

des dossiers passagers l'occasion d'étendre cette conception aux conventions internationales, comme l'illustre l'accord du 11 août 2012 entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure (sous-section 2). L'utilisation de l'adjectif sécuritaire renvoie ici à la sécurité publique dans le sens où l'utilisation des données des passagers aériens peut porter atteinte à cette dernière. Or, la sécurité publique est reconnue par le code de la sécurité intérieure comme un droit fondamental³⁶⁷. Ce droit est également consacré comme l'une des conditions de l'exercice des libertés individuelles et collectives.

Sous-section 1 – L'influence américaine originelle de l'usage sécuritaire des dossiers passagers

La mise en place du système PNR aux États-Unis a été précédée par l'essai de plusieurs systèmes qui utilisaient les données personnelles des passagers aériens à des fins répressives. À chaque fois, ces systèmes ont soulevé la protestation des organisations américaines en charge de la protection des droits individuels des citoyens américains.

§ 1 – Le système CAPPS : première initiative américaine

Avant même les attentats du 11 septembre 2001 et la signature du premier accord PNR entre Américains et Européens, les États-Unis avaient déjà fait usage des données personnelles des passagers aériens dans l'objectif de lutter contre le terrorisme. La mise en place du Computer-Assisted Passenger Prescreening System (CAPPS) a été l'une des premières initiatives sécuritaires qui mit au défi la protection des droits des passagers aériens américains³⁶⁸.

L'ancêtre du CAPPS, le système CAPS, a été développé dans un contexte politique déjà caractérisé par une criminalité internationale touchant l'aviation civile. L'événement le plus marquant à cet égard est l'attentat à la bombe qui a tué tous les passagers du vol 800 de Trans World Airlines. En effet, le 17 juillet 1996, un Boeing 747-100 a explosé quelques minutes après son décollage et s'est écrasé dans l'océan Atlantique près d'East Moriches, non loin de New York³⁶⁹. La Commission Gore, aussi connue comme la Commission de la Maison Blanche sur la sécurité et sûreté aérienne, a été créée à la suite du crash, le 22 août 1996, par le Executive Order 13015 pour répondre aux nouveaux défis ainsi posés à l'aviation civile américaine.

³⁶⁷ Code de la sécurité intérieure, article L. 111-1.

³⁶⁸ V. ALBERTO, D. BOGATZ, Computer Assisted Passenger Prescreening System ("CAPPS II"): National Security V. Civil Liberties, 19 mai 2004.

³⁶⁹ P. MUNTEAN, D. COLE, "25-year anniversary of TWA Flight 800 explosion marks new chapter in disaster's history", *CNN*, 18 juillet 2021.

En conséquence de cet attentat, la Federal Aviation Administration (FAA) a accordé une subvention à Northwest Airlines afin qu'elle développe un système de contrôle préventif³⁷⁰ assisté par ordinateur, débouchant sur le test d'un système prototype en 1996. En 1997, d'autres grands transporteurs ont également commencé à travailler avec des systèmes de contrôle. Par ailleurs, la plupart des compagnies aériennes basées aux États-Unis ont employé CAPS. La Commission Gore a publié son rapport final en février 1997, recommandant aux États-Unis de mettre en œuvre un système profilage pour ses aéroports³⁷¹.

Puis, le 19 avril 1999, la FAA a publié un avis de proposition de réglementation³⁷² (A Notice of Proposed Rulemaking - NPRM) concernant la sécurité des bagages enregistrés sur les vols à l'intérieur des États-Unis³⁷³. D'après ce document, les autorités supervisant les vols intérieurs aux États-Unis seraient tenues d'utiliser le système de filtrage des passagers assisté par ordinateur (CAPS), approuvé par la FAA, en vue de sélectionner ceux dont les bagages enregistrés doivent être soumis à des mesures de sécurité supplémentaires.

Rebaptisé CAPPs (Computer-Assisted Passenger Prescreening System), ce système est basé sur des règles qui utilisent les informations fournies par le passager lors de l'achat du billet pour déterminer s'il appartient à l'une des deux catégories suivantes : les « sélectionnés » qui passent un contrôle de sécurité supplémentaire et ceux qui ne le sont pas. Par ailleurs, le système CAPPs compare le nom du passager à ceux figurant sur une liste de terroristes connus ou suspects³⁷⁴.

Le concept opérationnel qui sous-tend ce dispositif consiste à sélectionner les voyageurs « à haut risque » en fonction de certaines caractéristiques identifiées dans les données des dossiers passagers. Il s'agit, entre autres, de prendre en considération les modes d'achat des billets et les détails des itinéraires de voyage. Ce système de vérification vise à permettre un examen plus approfondi en termes de contrôle des bagages pour certains passagers tout en accélérant la vérification des bagages pour les passagers « à faible risque ». En d'autres termes, ce dispositif a été conçu pour déterminer quels passagers étaient peu susceptibles

³⁷⁰ Bureau européen de Bruxelles, « Un code couleur pour cibler les passagers "à risques" », *Le Monde*, 21 juin 2004.

³⁷¹ White House Commission on Aviation Safety and Security: Final Report to President Clinton, 12 février, 1997.

³⁷² A Notice of Proposed Rulemaking (NPRM) est un document qui décrit et explique les règlements que le gouvernement fédéral propose d'adopter à une date future en invitant les parties intéressées à soumettre des commentaires à leur sujet. Ces commentaires peuvent ensuite être utilisés dans l'élaboration d'un règlement final.

³⁷³ Security of Checked Baggage on Flights Within the United States, *The Daily Journal of the of the United States Government*, Federal Register, A Proposed Rule by the Federal Aviation Administration on 04/19/1999.

³⁷⁴ Government Accountability Office, Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges 5-6, Rapport GAO-04-385, février, 2004.

d'avoir un engin explosif dans leurs bagages enregistrés, de sorte que les capacités limitées de détection d'explosifs puissent se concentrer sur un plus petit nombre de passagers et de bagages. Le système CAPPS n'est pas visible pour le public et le gouvernement fédéral est supposé ne pas contrôler ni collecter les données ainsi utilisées, car le système lui-même est intégré dans les systèmes de réservation des compagnies aériennes, comme Sabre.

Cependant, CAPPS s'est retrouvé au centre des débats qui ont suivi les attentats du 11 septembre 2001. En effet, la Commission nationale³⁷⁵ (ci-après Commission 9/11) mise en place après les attentats a révélé que neuf des dix-neuf terroristes avaient été sélectionnés pour un contrôle supplémentaire des bagages par le CAPPS³⁷⁶. Toutefois, les autorités américaines n'ont pas utilisé le dispositif pour un contrôle plus approfondi au niveau des points de contrôle des passagers, autrement dit aux portes d'embarquement. Or, ce contrôle est la principale mesure pour empêcher les détournements d'avions³⁷⁷. Son absence a conduit à ce qu'aucun des dix-neuf terroristes n'a été empêché de monter à bord d'un avion. Ayant montré des failles après les attentats 11 septembre 2001, le système a été appelé à être révisé.

§ 2 – CAPPS II : une tentative avortée de développement du système CAPPS

Le CAPPS II³⁷⁸ devait être la réponse apportée par les autorités américaines aux failles que les attentats du 11 septembre 2001 ont révélées. En effet, la Commission 9/11 a recommandé que les listes d'interdiction de vol et de sélection automatique soient améliorées et que les passagers aériens soient contrôlés non seulement par rapport à ces listes mais aussi à la lumière de l'ensemble des listes de surveillance détenues par le gouvernement fédéral³⁷⁹. Pour la Commission, cette mission incombait davantage à la Transportation Security Administration³⁸⁰ (ci-après TSA) qu'aux transporteurs aériens. Ces derniers devaient être

³⁷⁵ La commission nationale sur les attaques terroristes contre les États-Unis, également connue sous le nom de Commission du 11 septembre (National Commission on Terrorist Attacks Upon the United States ou 9/11 Commission) est une commission d'enquête parlementaire américaine qui a été mise en place en 2002 pour étudier les circonstances autour des attentats du 11 septembre 2001.

³⁷⁶ Statement of Cathal L. Flynn to the National Commission on Terrorist Attacks Upon the United States, Jan. 27, 2004, p. 4.

³⁷⁷ A. LEE, A.G. NIKOLAEV, S. JACOBSON, "Protecting air transportation: a survey of operations research applications to aviation security", *Journal of Transportation Security*, 2008.

³⁷⁸ A. BARNETT, "CAPPS II: the foundation of aviation security?", *Risk analysis: an official publication of the Society for Risk Analysis*, 2004.

³⁷⁹ National Commission on Terrorist Attacks Upon the United States, the 9/11 Commission Report, Authorized ed. (New York: W.W Norton & Co., 2004), p. 393.

³⁸⁰ La Transportation Security Administration (TSA) est une agence gouvernementale créée dans le cadre de l'Aviation and Transportation Security Act de 2001. Initialement organisée au sein du département américain des transports, elle a été transférée au département américain de la sécurité intérieure le 25 novembre 2002. L'agence est responsable de la sécurité dans tous les modes de transport.

tenus de fournir les informations nécessaires pour tester le système de contrôle préventif des passagers aériens³⁸¹.

Ainsi, TSA a conçu CAPPs II comme « un système renforcé pour authentifier l'identité des passagers et identifier les terroristes étrangers ou les personnes ayant des liens avec une entreprise terroriste, avant de pouvoir embarquer dans les avions américains »³⁸². Ce système devait envoyer aux fournisseurs de données commerciales les données personnelles fournies par le passager, à des fins de comparaison et d'authentification de son identité. Celles-ci comprennent le nom complet, l'adresse, le numéro de téléphone et la date de naissance. Le fournisseur de données commerciales était ensuite appelé à adresser une évaluation numérique à TSA indiquant le niveau de risque que peut représenter le passager scanné³⁸³. Les passagers avec un score « vert » passaient par un « contrôle normal » tandis que les passagers avec un score « jaune » devaient passer un contrôle supplémentaire. Les passagers avec un score « rouge », quant à eux, n'étaient pas autorisés à embarquer sur le vol et étaient susceptibles d'être interrogés par les autorités compétentes³⁸⁴.

Alors que la TSA avait prévu de tester le système dans des aéroports sélectionnés au printemps 2004, le projet CAPPs II rencontra plusieurs obstacles qui compliquèrent sa mise en œuvre³⁸⁵. Le premier défi concernait l'obtention de données nécessaires pour tester le système. Plusieurs polémiques médiatisées ont entraîné des recours collectifs devant le juge américain, dissuadant ainsi les compagnies aériennes basées aux États-Unis de fournir volontairement des informations sur les passagers. Au début de l'année 2003, Delta Airlines devait commencer à tester CAPPs II en utilisant les données passagers de ses clients dans trois aéroports nationaux. Pourtant, ladite entreprise est devenue la cible d'une campagne de boycott retentissante³⁸⁶ mettant en avant les préoccupations des citoyens américains vis-à-vis de la protection de leurs données personnelles dans le cadre du projet CAPPs II.

Cette polémique sera suivie d'autres. En septembre 2003, la presse américaine a révélé que JetBlue avait partagé les données personnelles des dossiers passagers en septembre 2002 avec Torch Concepts, une entreprise spécialisée dans les questions de défense qui testait une

³⁸¹ Ibidem

³⁸² Transportation Security Administration, "TSA's CAPPs II Gives Equal Weight to Privacy, Security," Press Release, 11 mars 2003.

³⁸³ A. BARNETT, "CAPPs II: The Foundation of Aviation Security?", *Risk Analysis*, Volume 24, Issue 4, pp. 909-916, 2004. Voir R. O'HARROW, "JR., Aviation ID System Stirs Doubt", *Washington Post*, 14 mars 2003.

³⁸⁴ Transportation Security Administration, "TSA's CAPPs II Gives Equal Weight to Privacy, Security," Press Release, 11 mars 2003.

³⁸⁵ S. E. MARTONONSI, A. BARNETT, "How Effective Is Security Screening Of Airline Passengers?", *Interfaces*, 36(6), 2006, pp. 545-552. Voir. S. KEHAULANI GOO, "U.S. to Push Airlines for Passenger Records", *Washington Post*, 12 janvier, 2004.

³⁸⁶ H. CLIFTON, "Coverage focuses on criticism – not creation – of CAPPs II", *PRWeek*, 21 avril 2003.

application d'exploration de données pour l'armée américaine. Les informations partagées auraient inclus des itinéraires, des noms, des adresses et des numéros de téléphone de 1,5 million de passagers³⁸⁷. En janvier 2004, il a été rapporté que Northwest Airlines avait fourni, entre octobre et décembre 2001, des informations personnelles sur des millions de ses passagers à la National Aeronautics and Space Administration (NASA) pour une mission d'exploration de données liée à la sécurité des compagnies aériennes³⁸⁸.

En avril 2004, ce sera au tour d'American Airlines d'être prise dans le tourbillon des polémiques autour de l'utilisation des données personnelles des passagers aériens. En effet, la presse américaine a révélé que la compagnie américaine a accepté de fournir des données personnelles de dossiers passagers de 1,2 million de ses clients à la TSA en juin 2002³⁸⁹. D'autres exemples de données fournies dans le but de tester CAPPs II ont été dévoilés, le 23 juin 2004, lors d'une audience de confirmation des charges du Comité sénatorial des affaires gouvernementales. Dans ses réponses au comité, le directeur par intérim de la TSA, David M. Stone, a déclaré qu'en 2002 et 2003, quatre compagnies aériennes (Delta, Continental, America West et Frontier) et deux sociétés de réservation de voyages (Galileo International et Sabre Holdings) avaient fourni des données de dossiers passagers à la TSA et à ses sous-traitants³⁹⁰.

Outre les préoccupations liées à l'utilisation, irrégulière, des données personnelles des dossiers passagers, la réforme de ce système s'est heurtée à une difficulté liée aux types de passagers qui devaient être filtrés. En effet, le système CAPPs II était à l'origine destiné à filtrer uniquement les passagers à haut risque susceptibles de constituer une menace pour la sécurité des États-Unis. Or, dans un avis du Federal Register du 1^{er} août 2003, la TSA a déclaré que le CAPPs II pouvait également être utilisé pour identifier des individus sous mandat d'arrêt étatique ou fédéral en cours ainsi que des terroristes étrangers et nationaux, indiquant de ce fait explicitement que le système avait une portée extraterritoriale. L'avis mentionna également que CAPPs II pouvait être « lié au programme US Visitor and Immigrant Status Indicator Technology (US-VISIT) » visant à identifier les personnes qui se trouvent illégalement dans le pays³⁹¹. C'est le cas, par exemple, des personnes dont le visa a expiré ou des étrangers en situation irrégulière. Face à un grand nombre de critiques

³⁸⁷ D. PHILLIPS, "JetBlue Apologizes for Use of Passenger Records", *Washington Post*, 20 septembre 2003.

³⁸⁸ S. TAYLOR, "Big brother and another overblown privacy scare", *National Journal*, 2002. Voir S. KEHAULANI GOO, "Northwest Gave U.S. Data on Passengers", *Washington Post*, 18 Janvier 2004.

³⁸⁹ S. KEHAULANI GOO, "American Airlines Revealed Passenger Data", *Washington Post*, 10 avril 2004.

³⁹⁰ U.S. Senate Committee on Governmental Affairs Pre-hearing Questionnaire For the Nomination of Admiral David Stone to be Assistant Secretary of Homeland Security, Transportation Security Administration, 2004

³⁹¹ 68 Fed. Reg. 45266 (Aug. 1, 2003), GAO, Aviation Security: Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System 17 (GAO-04-504T), 17 mars 2004.

reprochant l'éloignement du système de sa mission initiale, la TSA a considéré que les utilisations suggérées étaient conformes aux objectifs d'amélioration de la sécurité aérienne³⁹².

Ces déclarations n'ont pas suffi à éteindre les inquiétudes de la société civile³⁹³. Plusieurs autres préoccupations ont d'ailleurs été soulevées, notamment quant à la durée pendant laquelle les informations sur les passagers devaient être conservées, l'accès à ces informations, l'exactitude des données commerciales utilisées pour authentifier l'identité d'un passager, la création de procédures permettant aux passagers de corriger les erreurs de données dans leurs dossiers et la capacité du système à repérer les tentatives, par des individus, d'utiliser le vol d'identité pour monter à bord d'un avion sans être détectés. En août 2004, la TSA a ainsi annoncé que le programme CAPPs II était supprimé et remplacé par un nouveau système appelé « Secure Flight ».

Les préoccupations concernant la protection des données personnelles des passagers aériens avaient également inquiété l'Union européenne qui, à travers l'accord PNR, devait fournir des données à la TSA pour tester CAPPs II. Or, en mai 2004, en signant un accord avec les États-Unis, les Européens ont autorisé l'utilisation des données PNR pour les vols en provenance de l'Union européenne dans le cadre des tests CAPPs II mais seulement après que la TSA a été autorisée à utiliser leurs données nationales des passagers européens. Dans le cadre de l'accord, les données des citoyens européens ne devaient être conservées que pendant trois ans et demi, sauf si elles relevaient d'une action répressive et seuls 34 des 39 éléments du PNR devaient être consultés par les autorités. Il était également prévu des examens conjoints annuels DHS-UE sur la mise en œuvre de l'accord³⁹⁴.

§ 3 – Le programme *Secure Flight* : une alternative sécuritaire

Après l'annulation du programme CAPPs II en 2004, la TSA a annoncé son remplacement par un nouveau système dénommé « Secure Flight », un programme géré par la Transportation Security Administration du DHS. Ce programme comparait les informations sur les passagers fournies par les compagnies aériennes aux listes de surveillance du gouvernement afin de détecter les voyageurs présents sur une liste d'interdiction de vol et les

³⁹² Ibidem

³⁹³ American Civil Liberties Union, “The Five Problems With CAPPs II: Why the Airline Passenger Profiling Proposal Should Be Abandoned”, *American Civil Liberties Union*, 2004.

³⁹⁴ K. PROPP, “Avoiding the Next Transatlantic Security Crisis: The Looming Clash Over Passenger Name Record Data”, *Atlantic Council*, 2021, en ligne à URL : https://www.atlanticcouncil.org/wp-content/uploads/2021/07/Avoiding-the-Next-Transatlantic-Security-Crisis-The-Looming-Clash-over-Passenger-Name-Record-Data_Final.pdf consulté le 3 octobre 2023. Voir. Department of Homeland Security, “Fact Sheet: US-EU Passenger Name Record Agreement Signed”, 28 mai 2004.

empêcher ainsi de monter à bord d'un avion. Le dispositif permettait d'identifier les personnes nécessitant un contrôle supplémentaire³⁹⁵.

Ce programme a dû franchir plusieurs obstacles avant d'être adopté par le législateur américain³⁹⁶. En effet, dans la loi de 2005 sur les crédits du Département de la sécurité intérieure³⁹⁷, le Congrès a intégré dans l'article 522 une disposition interdisant l'utilisation des fonds affectés au développement de programmes tels que CAPPS II, Secure Flight et d'autres. Cependant, le Government Accountability Office³⁹⁸ (ci-après GAO) a certifié qu'un tel système avait satisfait à toutes les exigences de protection de la vie privée énumérées dans un rapport du GAO de février 2004³⁹⁹. Le rapport de certification du GAO a été remis au Congrès en mars 2005. Dans ce dernier, l'organisme américain d'audit et d'évaluation des comptes publics a constaté que, nonobstant les améliorations que le programme Secure Flight présentait, certaines failles dans le développement du programme existaient encore, l'empêchant de répondre aux exigences de protection de la vie privée prévues par le Congrès⁴⁰⁰⁴⁰¹. À l'aube de 2006, la TSA a donc suspendu le développement du programme Secure Flight dans le but de le réévaluer.

En décembre 2006, le Privacy Office du DHS, en charge de l'évaluation des politiques de protection de la vie privée, a publié un rapport comparant les études sur la protection de la vie privée (Privacy Notice) publiées par la TSA et la pratique du programme de Secure Flight en la matière. Il a alors été constaté qu'il existait des divergences liées au traitement et à la conservation des données, dues en partie au fait que les Privacy Notice « ont été rédigées avant que le programme testé n'ait été entièrement conçu »⁴⁰².

³⁹⁵ US Department Homeland Security, Privacy Impact Assessment Update for Secure Flight DHS/TSA/PIA-018(h), 12 juillet 2017.

³⁹⁶ P. CARSTENSEN, "The Lamppost, the Wizard, and the Law: Reflections on Professor Barnett's Assessment of CAPPS II", *Risk Analysis*, 2004.

³⁹⁷ Department of Homeland Security Appropriations Act, 2005.

³⁹⁸ Organisme d'audit, d'évaluation et d'investigation du Congrès des États-Unis chargé du contrôle des comptes publics du budget fédéral des États-Unis. Il fait partie de la branche législative du gouvernement fédéral des États-Unis. Cet organisme est dirigé par le Contrôleur général des États-Unis (Comptroller General of the United States).

³⁹⁹ I. RAVID. "Safety Versus Defense: Comments on "CAPPS II: The Foundation of Aviation Security?", *Risk Analysis*, 2004. GAO, Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385, 2004.

⁴⁰⁰ L. A. MCLAY, "Risk-Based Resource Allocation Models for Aviation Security", in *Safety and Risk Modeling and Its Applications*, pp. 243-261, 2011. Voir GAO, Aviation Security: Significant Management Challenges May Adversely Affect the Implementation of the Transportation Security Administration's Secure Flight Program (GAO-06-374T), 2006.

⁴⁰¹ L. A. MCLAY, S. H. JACOBSON, J. E. KOBZA, "The tradeoff between technology and prescreening intelligence in checked baggage screening for aviation security", *Journal of Transportation Security*, pp.107-126, 2008. GAO, Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program (GAO-06-864T), 2006.

⁴⁰² US Department Homeland Security, Secure Flight Report, DHS Privacy Office Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations, December 2006

Un autre apport de ce rapport réside dans la préconisation de ses auteurs relative à la conception de ce programme. En effet, ces derniers ont considéré qu'un tel projet fédéral, ayant un impact sur la collecte, l'utilisation et le traitement de données personnelles de citoyens américains, devait être explicitement annoncé dans le projet de loi comme dans tous les autres documents concernés⁴⁰³.

Or, cela ne semblait pas avoir été explicitement évalué. Ces difficultés à atteindre un niveau suffisant vis-à-vis des exigences des autorités américaines, en matière de protection des données personnelles des passagers aériens, persisteront quelques années. C'est ce qui avait poussé le directeur de la TSA, Kip Hawley, à déclarer que cette amélioration ne serait pas effective avant un an et demi, quand bien même la TSA a développé un moyen d'améliorer le programme Secure Flight, notamment au sujet de la protection des données personnelles. Celle-ci a pris une année supplémentaire de tests et n'a donné lieu à une mise en œuvre qu'en 2010⁴⁰⁴. Par ailleurs, le législateur américain, à travers l'article 522 (a) de la loi de 2005 sur les crédits du Département de la sécurité intérieure, avait posé dix conditions pour l'élaboration et la mise en œuvre du programme Secure Flight que le secrétaire à la Sécurité intérieure doit certifier avoir été remplies avec succès avant que le programme ne puisse être mis en œuvre, excluant le déploiement à titre d'essai⁴⁰⁵.

Les promoteurs du programme Secure Flight devaient, d'une part, assurer une protection des données personnelles des citoyens américains et répondre aux exigences du législateur américain et, d'autre part, identifier les risques qui peuvent fragiliser la protection de la vie privée des passagers aériens que les observateurs avaient relevés⁴⁰⁶. C'est à cette fin que Secure Flight a intégré dans son programme l'exigence de nommer un responsable de la protection de la vie privée (Privacy Officer) accompagné d'une équipe d'experts en matière de protection des données personnelles. Ce dernier travaille en étroite collaboration avec ses homologues de la TSA et DHS afin d'identifier les risques et les stratégies d'anticipation appropriées.

Depuis 2007, les équipes de Secure Flight ont publié huit rapports qui intègrent, notamment, l'analyse d'impact relative à la protection des données (PIA, Privacy Impact Assessment), en coordination avec le DHS. Ces études incorporent les différentes mises à jour concernant les

⁴⁰³ "Material changes in a federal program's design that have an impact on the collection, use, and maintenance of personally identifiable information of American citizens are required to be announced in Privacy Act system notices and privacy impact assessments".

⁴⁰⁴ E. LIPTON, "U.S. Official Admits to Big Delay in Revamping No-Fly Program", *New York Times*, 21 février 2007.

⁴⁰⁵ Department of Homeland Security Appropriations, 2005.

⁴⁰⁶ ACLU, The four biggest problems with the "secure flight" airline security program, 2005.

évaluations des risques générées par l'activité aérienne et le traitement des données personnelles des passagers aériens⁴⁰⁷. Ces mises à jour montrent que le programme Secure Flight permet des vérifications par rapport aux listes de surveillance des documents de voyage perdus et volés, y compris les passeports internationaux.

Sous-section 2 – Un accord euro-américain essentiellement sécuritaire

L'accord PNR entre les États-Unis et l'Union européenne se caractérise par l'affirmation de l'utilisation des données personnelles des passagers aériens à des fins répressives. Cette vocation est le résultat de l'influence américaine dans la conclusion de cet accord.

§ 1 – L'état d'esprit de l'accord : une vision américaine répressive confirmée

L'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure a été publié au journal officiel du 11 août 2012⁴⁰⁸. Comme il a été rappelé dans le premier chapitre, cet accord a été le fruit d'après négociations entre les autorités européennes et américaines durant lesquelles l'Union européenne a tenté de remédier à l'unilatéralisme des États-Unis.

Pour autant l'emprise américaine, axée sur la sécurité⁴⁰⁹, reste prégnante à la lecture de l'accord. Elle se retrouve dès les premiers considérants de son préambule qui mettent l'accent sur l'aspect sécuritaire de l'accord entre Américains et Européens quant à l'utilisation des données PNR. Le premier rappelle, en effet, que les deux parties désirent « prévenir et combattre efficacement le terrorisme et les formes graves de criminalité transnationale afin de protéger leurs sociétés démocratiques respectives et les valeurs qui leur sont communes »⁴¹⁰, en reconnaissant, dans le troisième considérant, « le droit et la responsabilité des États d'assurer la sécurité de leurs citoyens et de protéger leurs frontières, et ayant à l'esprit la responsabilité de toutes les nations de protéger la vie de la population en veillant à sa sûreté, y compris des personnes utilisant les systèmes de transport international ». Dans le quatrième considérant, les deux pays signataires de l'accord sont « convaincus que le partage d'informations est une composante essentielle de la lutte contre le terrorisme et les formes graves de criminalité transnationale et que, dans ce contexte, le traitement et l'utilisation des

⁴⁰⁷ US Department Homeland Security, Privacy Impact Assessment Update for Secure Flight DHS/TSA/PIA-018(h), 12 juillet 2017.

⁴⁰⁸ Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au Ministère américain de la sécurité intérieure, *Journal officiel* n° L 0215 du 11/08/2012, p. 5.

⁴⁰⁹ J. POIROT, « PNR (Passenger Name Record) », in *Dictionnaire du renseignement*, 2018, pp. 611-613. Voir aussi. L. IDOT, « Vers une Union de la sécurité », *Europe* n° 11, alerte 57, novembre 2017.

⁴¹⁰ Accord PNR, considérant 1.

dossiers passagers (Passenger Name Record ou PNR) constituent des instruments nécessaires qui permettent d'avoir accès à des informations ne pouvant être obtenues par d'autres moyens ». Enfin, selon le cinquième considérant, ce partage d'information est essentiel pour « prévenir et combattre les infractions terroristes et la criminalité transnationale, tout en respectant les droits et libertés fondamentaux et en reconnaissant l'importance du droit au respect de la vie privée et à la protection des données et informations à caractère personnel »⁴¹¹.

La mention de la question de la protection des droits et libertés fondamentaux seulement au cinquième considérant de l'accord, après de multiples références à des thèmes sécuritaires, n'est pas anodine : elle reflète l'état d'esprit avec lequel sont abordées les données des passagers dans cet accord, à savoir une conception sécuritaire largement inspirée par les premières initiatives américaines d'utilisation des données personnelles des passagers aériens précédemment exposées, notamment le CAPPS⁴¹². Le deuxième et troisième considérant se distinguent par des mentions liées à l'aspect international⁴¹³ et extraterritorial de l'utilisation des données passagers. Ces mentions renvoient au contexte particulier de mise en œuvre de l'accord PNR entre les États-Unis d'Amérique et l'Union européenne, puisque ce sont les attentats terroristes du 11 septembre 2001 qui ont enclenché la dynamique de développement de l'utilisation des données personnelles des passagers pour des raisons sécuritaires.

Ainsi, les cinq premiers considérants de l'accord reflètent l'état d'esprit qui animait ses rédacteurs avec une multiplication des références marquant une volonté de réprimer le terrorisme et la criminalité transnationale en utilisant les données des dossiers passagers. Ces considérants traduisent un rapport de force au bénéfice des États-Unis : on peut y déceler la prédominance⁴¹⁴ de la vision sécuritaire américaine relative à l'utilisation des données des dossiers passagers (données PNR), l'accord prévoyant leur transfert au ministère américain de la sécurité intérieure. Cette vision sécuritaire se manifeste concrètement par une volonté affichée de privilégier la sécurité publique⁴¹⁵.

⁴¹¹ Accord PNR, considérant 5.

⁴¹² Computer-Assisted Passenger Prescreening System.

⁴¹³ P. DU BOIS, « L'Union européenne et les droits de l'homme », *Relations internationales*, 2007, pp. 33-39. Voir aussi R. TINIÈRE, « Droits fondamentaux et exception en droit de l'UE : dialectique entre intégration et désintégration », in *L'exception en droit de l'Union européenne*, 2019, pp. 337-346.

⁴¹⁴ P. BERTHELET, « Tous les chemins mènent... à Luxembourg. Analyse institutionnelle de l'accord PNR UE-Canada », *RDLF*, chron. n° 20, 2018. Voir aussi J. HARIVEL, *Libertés publiques, libertés individuelles, risques et enjeux de la société numérique*, Thèse, Université Panthéon-Sorbonne – Paris 1, 2018.

⁴¹⁵ J. AUVRET-FINCK, « L'échange d'information dans les accords PNR conclus par l'Union européenne avec des États tiers », in C. Chevallier-Govers (dir.), *L'échange des données dans l'espace de liberté, de sécurité et de justice de l'Union européenne*, Mare & Martin, coll. « Droit public », 2017, p. 269. Voir aussi S. PEYROU, « La protection des données personnelles face aux programmes PNR. Une illustration du difficile équilibre entre lutte

Les autres considérants permettent aux rédacteurs de l'accord de mettre en avant l'un des principaux acteurs du système PNR : le DHS⁴¹⁶ américain, cité plusieurs fois. Cette récurrence confirme l'importance de la vocation sécuritaire des accords PNR et l'empreinte américaine. Toutefois, on trouve le besoin, pour les rédacteurs de l'accord, de rappeler dans le neuvième considérant que « les traditions de longue date des deux parties de respect de la vie privée des personnes, comme le reflètent leurs législations et actes fondateurs »⁴¹⁷. Or le constat que « le DHS traite et utilise les dossiers passagers à des fins de prévention et de détection d'infractions terroristes et de la criminalité transnationale, ainsi que d'enquêtes et de poursuites en la matière [...] » témoigne de la volonté des rédacteurs d'acter, d'une certaine manière, la primauté de la protection de la collectivité sur celle de l'individu, bien que ce constat soit suivi par l'affirmation selon laquelle ce traitement se fait « dans la stricte observation des garanties relatives au respect de la vie privée et à la protection des données et informations à caractère personnel, telles qu'énoncées dans le présent accord ». Puis, dans son onzième considérant, l'accord affirme le besoin de protéger les données personnelles des passagers aériens : « le DHS utilise actuellement des procédures fiables pour protéger la vie privée des personnes et garantir l'intégrité des données, se rapportant notamment à la sécurité physique, aux contrôles d'accès, au chiffrement et à la séparation des données, aux capacités d'audit et aux mesures effectives de responsabilisation »⁴¹⁸. Cette préoccupation est réitérée dans le quinzième considérant en ces termes : « le DHS est réputé garantir un niveau adéquat de protection des données pour le traitement et l'utilisation des dossiers passagers qui lui sont transférés »⁴¹⁹ ; il est mis en avant « la bonne conduite » du DHS, montrant tacitement une volonté d'écarter les accusations qui ont prévalu lors de la signature de l'accord, considérant que l'Union européenne « bradait » les droits des citoyens européens⁴²⁰.

Les dixième et seizième considérant rappellent que l'approche européenne, exprimée notamment à travers les arrêts de la Cour de justice de l'Union européenne, a permis d'intégrer dans l'accord des références juridiques liées aux libertés fondamentales malgré le rapport de force imposé par les Américains. Le seizième considérant indique aussi que les deux parties ont « à l'esprit » que « les États-Unis et l'Union européenne s'engagent à garantir

contre le terrorisme et protection des droits fondamentaux », in *Mélanges en l'honneur du Professeur Pierre Bon*, Dalloz, 2014, p. 487.

⁴¹⁶ Department of Homeland Security.

⁴¹⁷ Accord PNR, considérant 9.

⁴¹⁸ Accord PNR, considérant 11.

⁴¹⁹ Accord PNR, considérant 15.

⁴²⁰ S. PEYROU, « La protection des données personnelles face aux programmes PNR. Une illustration du difficile équilibre entre lutte contre le terrorisme et protection des droits fondamentaux », op. cit., p. 48. Voir aussi. L. CHECOLA, « L'UE approuve le transfert aux USA des données des passagers européens », *Le Monde*, 19 avril 2012.

un niveau élevé de protection des informations à caractère personnel dans le cadre de la lutte contre la criminalité et le terrorisme »⁴²¹. L'emploi de l'expression « informations personnelles » au lieu de « données personnelles » interpelle puisque cette différence notionnelle n'est pas anodine. En effet, il rappelle la différence de culture juridique qui sous-tend les deux systèmes juridiques investis dans cet accord. Ce point s'ajoute à un autre élément notionnel distinctif qui marque la relation euro-américaine : le Right to Privacy⁴²², d'un côté ; les données personnelles et la vie privée, de l'autre. Du point de vue américain, le Right to Privacy renvoie à une liberté publique dont l'objectif est la limitation de l'État puisque la philosophie politique qui influence le quatrième amendement américain part du présupposé qu'il constitue une menace pour les libertés publiques.

Cette menace s'est accentuée avec le terrorisme qui s'est développé au début du siècle, à l'origine des mesures qui dépassent le champ de bataille⁴²³ et s'étendent dans le domaine juridique en fragilisant les libertés fondamentales. Ainsi, des citoyens non-américains résidant aux États-Unis ont été détenus par les autorités américaines en secret. D'autres, capturés en Afghanistan, ont été maintenus dans une base militaire extraterritoriale, à Guantanamo, et ont été privés de conseils juridiques ainsi que des droits garantis par le droit constitutionnel local mais également par le droit humanitaire international. Certains juristes américains ont dénoncé l'exercice du droit au silence tandis que d'autres ont soutenu le recours à la torture⁴²⁴.

L'accord en lui-même est venu entériner la dynamique transnationale⁴²⁵ du droit américain, notamment d'un dispositif répressif de lutte contre le terrorisme⁴²⁶ lancé par un gouvernement américain « en guerre », pour emprunter sa terminologie, au-delà de ses frontières⁴²⁷. Cependant, une autre dynamique juridique est en jeu, d'un point de vue national comme international, à propos de l'équilibre à trouver entre la sécurité de l'individu et celle de la

⁴²¹ Accord PNR, considérant 16.

⁴²² A. ALIBEIGI, A. MUNIR, M. KARIM, "Right to Privacy, A Complicated Concept to Review", *SSRN Electronic Journal*, 2019.

⁴²³ A. PLAW, "Targeting Terrorists. A Licence to Kill?", *Aldershot*, Ashgate, 2008, pp. 190 et s.

⁴²⁴ "Alan Dershowitz is Wrong about Torture, Again", *Human Rights First*, 19 septembre 2014.

⁴²⁵ K. TUORI, « Vers une théorie du droit transnational », *Revue internationale de droit économique*, 2013, pp. 9-36. Pour l'auteur, ce concept de droit transnational va au-delà de la division entre droit international et droit national et se présente comme une réaction aux limites temporelles et spatiales de la souveraineté des États. Diverses critiques ont été adressées à l'encontre de ces ingérences au nom de « l'humanitaire » notamment la critique des « liberal wars ». Voir L. FREEDMAN, « The Age of Liberal Wars », *Review of International Studies*, 2005, pp. 93-107.

⁴²⁶ Selon N. BERMAN, la lutte contre le terrorisme correspond à la définition du conflit armé donnée par le Tribunal pénal international pour l'ex-Yougoslavie (TPIY) dans l'affaire Tadic. Voir "Privileging Combat? Contemporary Conflict and the Legal Construction of Law," *Columbia Journal of Transnational Law*, vol. 43, n° 1 (2004), pp. 32-33.

⁴²⁷ J. J. MEARSHEIMER, "Bound to Fail: The Rise and Fall of the Liberal International Order", *International Security*, pp. 7-50, 2019.

collectivité ou de l'État. Cette dynamique transparaît dans plusieurs considérants de l'accord, notamment le cinquième.

§ 2 – L'accord euro-américain : la sécurité du collectif devant celle de l'individu

Cet état d'esprit sécuritaire, présent dès le préambule du texte, est confirmé dans son premier article qui affirme en effet que « l'accord a pour objet de garantir la sécurité et de protéger la vie de la population en veillant à sa sûreté »⁴²⁸. La place centrale de la sécurité consacrée dès le début marque l'insistance des rédacteurs, essentiellement des Américains, à insister sur la vocation sécuritaire des dossiers passagers puisqu'il est question de « sécurité », de « protection » et de « sûreté ». La multiplication des référentiels liés à la sécurité collective de la Nation ne laisse guère de place aux malentendus : les dossiers passagers ont pour objet de soutenir la dynamique sécuritaire née après les attentats du 11 septembre qui ont eu lieu de l'autre côté de l'Atlantique.

Toutefois, les rédacteurs n'ont jamais perdu de vue le jeu d'équilibre⁴²⁹ qui a marqué les débats autour de l'accord et surtout l'insistance des institutions européennes⁴³⁰, notamment du Parlement européen, à ne pas marginaliser les droits des individus, notamment en matière de protection des données personnelles. C'est en ce sens que le deuxième alinéa de l'article 1^{er} de l'accord mentionne « les responsabilités des parties à l'égard des conditions dans lesquelles les dossiers passagers peuvent être transférés, traités et utilisés, et protégés »⁴³¹, présageant ainsi que l'accord implique des obligations envers les États-Unis et l'Union européenne dans le traitement, l'utilisation, le transfert et la protection des dossiers passagers. Cet alinéa est également une preuve que l'Union européenne a pu « peser » dans le rapport de forces avec

⁴²⁸ Accord PNR, article 1.

⁴²⁹ L'encadrement juridique des données personnelles au sein des pays de l'Union européenne est constamment sujet à un débat épineux sur l'équilibre entre l'utilité de leur utilisation et la nécessité de les protéger. En Espagne, l'encadrement des données ouvertes a également été marqué par ces mêmes débats. Voir en ce sens. J. VALERO TORRIJOS & M. ANDREU MARTINEZ, « L'encadrement juridique des données ouvertes en Espagne, *Revue française d'administration publique*, 2018/3 N°167, pp.601-611.

⁴³⁰ Dès 2007, et à plusieurs reprises, le G29 va remettre en cause la nécessité et la proportionnalité des transferts de données PNR vers le sol américain. Voir : Avis 5/2007 concernant le nouvel accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au Ministère américain de la sécurité intérieure conclu en juillet 2007 (01646/07/EN, WP 138) et Avis 4/2003 sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers (11070/03/EN, WP 78) ; Avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers (622/10/EN, WP 178) ; Avis 10/2011 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers 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 (00664/11/EN, WP 181) ; Avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif du 27 février 2014 (536/14/FR, WP 211).

⁴³¹ Ce deuxième alinéa énonce : « À cette fin, le présent accord énonce les responsabilités des parties à l'égard des conditions dans lesquelles les dossiers passagers peuvent être transférés, traités et utilisés, et protégés ».

les États-Unis. Cependant, celle-ci a été insuffisante car le premier alinéa ne réserve l'objet de l'accord qu'à la triptyque « sécurité », « protection de la vie » et « sûreté ». La locution adverbiale « à cette fin » dans le deuxième alinéa de l'article 1^{er} permet aux rédacteurs mentionner les « instruments », parmi lesquels figure la protection des dossiers passagers, mis à disposition pour atteindre un objectif avant tout sécuritaire.

L'accord euro-américain sur les dossiers passagers s'applique « aux transporteurs assurant des services de transport de passagers entre l'Union européenne et les États-Unis »⁴³² et « aux transporteurs constitués en sociétés ou stockant des données dans l'Union européenne et assurant des services de transport de passagers au départ et à destination des États-Unis »⁴³³. Ainsi, d'après l'accord, si une compagnie aérienne exploite un vol à destination ou en provenance des États-Unis sans pour autant avoir de liens avec l'UE, elle y est tout de même assujettie dans la mesure où elle traite des données personnelles dans l'UE. À cet égard, le DHS assure qu'il filtre les vols, qui n'ont pas de lien avec les États-Unis, en utilisant les numéros de vol et les codes d'aéroport⁴³⁴.

Néanmoins, le DHS peut également collecter des données personnelles des passagers aériens qui prennent un vol sans lien avec les États-Unis. Cette collecte se produit en raison d'une prérogative du DHS consistant à obtenir des données PNR des passagers sur des vols qui n'ont pas de lien avec les États-Unis au cas où ces vols atterriraient sur le sol américain pour des raisons imprévues. En fait, il s'agit de l'un des scénarios exceptionnels dans lesquels les autorités américaines peuvent accéder directement aux systèmes de réservation des compagnies aériennes⁴³⁵. Cette prérogative est prévue par l'article 17 de l'accord sous l'intitulé « Transfert ultérieur ».

§ 3 – Des finalités sécuritaires de l'accord affirmées

L'analyse de l'article 4 de l'accord⁴³⁶ PNR est essentielle, puisqu'elle permet de comprendre les finalités pour lesquelles les données personnelles des passagers aériens sont collectées, utilisées et traitées. La ligne générale est claire : les États-Unis « recueillent, utilisent et traitent les dossiers passagers à des fins de prévention et de détection des infractions visées ci-après, ainsi que d'enquêtes et de poursuites » telles que « les infractions terroristes et infractions pénales qui y sont liées » ainsi que « les autres infractions passibles d'une peine

⁴³² Accord PNR, article 2 (2).

⁴³³ Accord PNR, article 2 (3).

⁴³⁴ Commission européenne, Report from the Commission to the European Parliament and the Council, Bruxelles, 19 janvier 2017.

⁴³⁵ Ibidem

⁴³⁶ Accord PNR, article 4.

d'emprisonnement d'au moins trois années et de nature transnationale ». En outre, l'article 4 mentionne d'autres hypothèses dans lesquelles le DHS peut utiliser et traiter les données personnelles des passagers aériens⁴³⁷.

L'article 4 (1) (a) (i) de l'accord définit les infractions terroristes et infractions pénales comme « tout comportement qui 1) implique des actes violents ou dangereux pour la vie humaine, les biens, ou les infrastructures et 2) apparaît comme destiné : a) à intimider ou contraindre une population civile; b) à influencer la politique d'un gouvernement par l'intimidation ou la coercition; ou c) à nuire à l'action d'un gouvernement par la destruction de masse, l'assassinat, l'enlèvement ou la prise d'otages; » et « ii) tout acte qui constitue une infraction au sens et selon la définition des conventions et protocoles internationaux applicables relatifs au terrorisme; »⁴³⁸.

Ces infractions terroristes, proposées par l'accord, diffèrent des infractions listées par la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme qui comprend dans son Titre II une liste des infractions terroristes et infractions liées à un groupe terroriste, et dans son Titre III, une liste des infractions liées à des activités terroristes plus complètes que celles présentées par l'accord.

Tout d'abord, la directive⁴³⁹ énumère une liste d'infractions comme les atteintes à la vie d'une personne pouvant entraîner la mort ou toutes atteintes à l'intégrité physique d'une personne, l'enlèvement ou la prise d'otage. Par exemple, le fait de causer des destructions massives à une installation gouvernementale ou publique, à un système de transport, à une infrastructure, y compris un système informatique. Sont également concernés les dommages causés à une plateforme fixe située sur le plateau continental, à un lieu public ou une propriété privée, susceptibles de mettre en danger des vies humaines ou de produire des pertes économiques considérables. Cela inclut aussi la capture d'aéronefs et de navires ou d'autres moyens de transport collectifs ou de marchandises. De même, la fabrication, la possession, l'acquisition, le transport, la fourniture ou l'utilisation d'explosifs ou d'armes, y compris d'armes chimiques, biologiques, radiologiques ou nucléaires sont des infractions graves. La recherche et le développement liés à ces armes, la libération de substances dangereuses ou la

⁴³⁷ Une réflexion critique sur la portée des attentats du 11 septembre 2001 et de la politique américaine est donnée par Alain Touraine : A. TOURAINE, *Un nouveau paradigme pour comprendre le monde d'aujourd'hui*, Fayard, 2005.

⁴³⁸ 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.

⁴³⁹ Ibidem.

provocation d'incendies, d'inondations ou d'explosions ayant pour effet de mettre en danger des vies humaines, sont également répertoriés comme des infractions dans la directive.

Dans la liste de ces infractions, on peut citer également la perturbation ou l'interruption de l'approvisionnement en eau, en électricité ou toute autre ressource naturelle fondamentale ayant pour effet de mettre en danger des vies humaines ainsi que l'atteinte illégale à l'intégrité d'un système. Elle est visée à l'article 4 de la directive 2013/40/UE du Parlement européen et du Conseil (19), dans les cas où l'article 9, paragraphe 3, ou l'article 9, paragraphe 4, point b) ou c), de ladite directive s'applique, et l'atteinte illégale à l'intégrité des données. Cette dernière est visée à l'article 5 de ladite directive, dans les cas où l'article 9, paragraphe 4, point c), de ladite directive s'applique, la menace de commettre l'un des actes énumérés aux points a) à i).

À cette liste d'infractions que les États membres doivent transposer dans leur droit national, s'ajoutent ensuite des infractions liées à un groupe terroriste, prévues à l'article 4 de l'accord PNR. En effet, les États signataires sont appelés à sanctionner, en tant qu'infractions pénales, « la direction d'un groupe » et « la participation aux activités d'un groupe terroriste, y compris en fournissant des informations ou des moyens matériels, ou par toute forme de financement de ses activités, en sachant que cette participation contribuera aux activités criminelles du groupe terroriste »⁴⁴⁰.

D'autres infractions ont été prévues par le législateur européen⁴⁴¹, au Titre III, telles que les infractions liées à des activités terroristes, comme par exemple la provocation publique à commettre une infraction terroriste, le recrutement pour le terrorisme, le fait de dispenser un entraînement au terrorisme, le fait de recevoir un entraînement au terrorisme, le voyage à des fins de terrorisme, le fait d'organiser ou de faciliter, de quelque autre manière, des voyages à des fins de terrorisme, le financement du terrorisme et les autres infractions liées à des activités terroristes⁴⁴².

Comparé aux infractions listées par la directive européenne, l'article 4 de l'accord euro-américain semble définir de manière extensive les infractions terroristes et les infractions liées

⁴⁴⁰ Accord PNR, article 4.

⁴⁴¹ S. DIMITROULIAS, « L'humanisme juridique européen à l'épreuve du terrorisme : le crépuscule de la clémence ? », *L'Homme & la Société*, 2006, pp. 111-132. Voir aussi M. DEN BOER, « 9/11 and the europeanisation of anti-terrorism policy: a critical assessment », *Groupe d'études et de recherches « Notre Europe »*, Paris, 2003 ; A. CRAWFORD (ed.), *Crime and insecurity: the governance and safety in Europe*, Cullompton, Willan, 2002.

⁴⁴² J. MONAR, « The European Union's Role in the Fight against International Terrorism: An Evaluation in the Light of the Response to 11 September 2001 », in Georges Vandensanden et Aline de Walsche (eds.), *Mélanges en hommage à Jean-Victor Louis*, Institut d'études européennes, Bruxelles, éd. de l'Université de Bruxelles, Bruxelles, vol. 1, 2003, pp. 335-354.

au terrorisme. En ce qui concerne la description des crimes transnationaux, cette disposition ne fait pas référence au for américain ; par conséquent, toute infraction impliquant plus d'un for peut être considérée comme transnationale même si cette infraction n'a aucun lien avec le for américain. Par ailleurs, ce même article reste silencieux sur la compétence juridique⁴⁴³ concernant le seuil de détermination de la peine pour les crimes transnationaux.

Ainsi, la définition de la criminalité transnationale dans le cadre de l'accord n'est pas précisée. En outre, l'article 4 autorise l'utilisation des données des dossiers passagers à des fins autres que la lutte contre le terrorisme telles que les contrôles aux frontières ou d'autres infractions. Ainsi, on constate que les contours des infractions prévues par l'accord euro-américain ne sont pas précis, créant une insécurité juridique pour les utilisateurs du transport aérien.

À travers sa conception extensive des infractions pénales, l'article 4 vient confirmer l'emprise de la lecture américaine de l'utilisation des dossiers passagers en conférant d'importants pouvoirs aux entités qui seront amenées à traiter, utiliser et transférer ces données personnelles des passagers aériens. En effet, une telle flexibilité, permettant une utilisation élargie des dossiers passagers, reflète la volonté américaine d'utiliser les données personnelles dans sa « lutte » contre le terrorisme et le crime transnational. Une comparaison de cet article avec les infractions pénales de la directive européenne relative à la lutte contre le terrorisme témoigne d'une différence de conception entre Européens et Américains s'agissant de la répression des actes terroristes. La priorité donnée à la lecture sécuritaire américaine dans la rédaction de ces infractions pénales traduit un rapport de force défavorable aux Européens.

§ 4 – Le transfert de données personnelles dans le cadre l'accord PNR euro-américain : l'avantage américain réaffirmé

L'article 15 (1) de l'accord PNR conclu entre les États-Unis et l'Union européenne a tranché la question du mode de transmission des dossiers passagers en affirmant que « les transporteurs doivent transférer au DHS les dossiers passagers en utilisant la méthode « push », conformément à la nécessité de faire en sorte que les dossiers passagers soient fiables, complets et fournis en temps opportun ». Il ajoute que ces transporteurs « doivent transférer les dossiers passagers au DHS par des moyens électroniques sécurisés dans le respect des exigences techniques du DHS ». L'accord PNR consacre ainsi le dispositif « push » comme la méthode de principe de transfert des données PNR. Toutes les compagnies

⁴⁴³ A. PETROPOULOU, *Liberté et sécurité : les mesures antiterroristes et la Cour européenne des droits de l'homme*, Editions A. Pedone, 2014, Paris.

aériennes devaient avoir la capacité technique d'utiliser cette méthode au plus tard le 1^{er} janvier 2014⁴⁴⁴. Jusqu'à cette date, le DHS était autorisé à accéder aux systèmes de réservation automatisés des compagnies aériennes qui n'avaient pas encore acquis de système permettant l'utilisation de la méthode « push ».

Toutefois, le DHS a conservé son droit d'accéder aux systèmes de réservation des compagnies aériennes même après le 1^{er} janvier 2014. Il peut donc exiger des compagnies aériennes qu'elles fournissent l'accès à leurs systèmes si elles ne sont pas en mesure d'envoyer des données PNR pour des raisons techniques. Cette possibilité permet l'utilisation de la méthode « pull » prévue par l'accord, où le DHS peut demander, au cas par cas, que les transporteurs fournissent les dossiers passagers en dehors des transferts réguliers. Lorsque les transporteurs ne peuvent pas répondre en temps utile aux demandes en raison de contraintes techniques, ou dans des circonstances exceptionnelles pour faire face à une menace spécifique, urgente et grave, ils sont tenus de fournir l'accès aux données d'une autre manière⁴⁴⁵.

Les compagnies aériennes sont tenues de fournir un tel accès entre ou après les transferts PNR prévus par la loi afin de répondre à une menace « spécifique, urgente et grave », lorsque des « circonstances exceptionnelles » l'exigent. L'accès aux données PNR doit être accordé au DHS, par exemple, dans le cas d'un vol sans lien avec les États-Unis si l'avion est contraint d'atterrir sur le sol américain en raison de conditions météorologiques exceptionnelles.

Certes, l'utilisation de la méthode « push » empêche potentiellement le DHS d'accéder aux données PNR sans autorisation. Cependant, le DHS peut toujours extraire les données PNR du système de réservation des compagnies aériennes dans certains cas exceptionnels. Par ailleurs, l'accord ne prévoit aucun mécanisme de révision en ce qui concerne ces cas exceptionnels dans lesquels la méthode « pull » est employée par le DHS. Cette méthode d'accès aux données PNR est donc laissée à la seule discrétion de ce dernier, d'où le risque d'un accès non autorisé soulevé par la doctrine⁴⁴⁶.

D'après l'article 3 de l'accord PNR, « les transporteurs fournissent au DHS les dossiers passagers figurant dans leurs systèmes de réservation, comme l'exigent les normes du DHS et conformément à celles-ci, et dans le respect du présent accord. Si les dossiers passagers transférés par les transporteurs contiennent des données autres que celles énumérées en

⁴⁴⁴ E.M. KUŞKONMAZ, *Privacy and Border Controls in the Fight against Terrorism*, Immigration and Asylum Law and Policy in Europe, 18 mars 2021.

⁴⁴⁵ Accord PNR, article 15.

⁴⁴⁶ E.M KUŞKONMAZ, *Privacy and Border Controls in the Fight against Terrorism*, op. cit.

annexe, le DHS les supprime dès qu'il les reçoit »⁴⁴⁷. Précisément, les transporteurs doivent fournir aux autorités américaines dix-neuf types de données de dossiers passagers listés dans un document annexé à l'accord PNR.

Les types de données PNR évoqués dans l'accord incluent le code repère du dossier passager (PNR)⁴⁴⁸, la date de réservation/d'émission du billet, les dates prévues du voyage, les noms, les informations disponibles sur les grands voyageurs et les programmes de fidélisation, les autres noms mentionnés dans le dossier passager (PNR), y compris le nombre de voyageurs figurant dans le dossier, toutes les coordonnées disponibles comprenant les informations sur la source, toutes les informations disponibles relatives au paiement/à la facturation, à l'exclusion des autres détails de l'opération liés à la carte de crédit ou au compte et n'ayant pas de lien avec l'opération relative au voyage, l'itinéraire de voyage pour le dossier passager (PNR) spécifique, l'agence de voyages et l'agent de voyages, les informations sur le partage de code, les informations PNR scindé ou divisé, le statut du voyageur y compris les confirmations et le statut d'enregistrement, les informations sur l'établissement des billets, y compris le numéro du billet, billets aller simple et données « Automated Ticket Fare Quote », le prix du billet, toutes les informations relatives aux bagages, les informations relatives au siège, y compris numéro du siège occupé, les remarques générales, y compris les données OSI, SSI et SSR, les informations APIS éventuellement recueillies, l'historique complet des modifications des données PNR énumérées aux points 1 à 18⁴⁴⁹.

Initialement, comme on l'a déjà relevé, les compagnies aériennes collectaient les données PNR à des fins proprement commerciales ; elles ne collectaient ainsi que les données dont elles avaient besoin⁴⁵⁰. Or, le PNR peut contenir environ soixante éléments de données de dossiers passagers. Avec l'implication de l'OACI⁴⁵¹ et le développement du système PNRGOV⁴⁵² qui vise à adopter un format commun pour les données PNR, les catégories requises dans l'accord et celles collectées dans la pratique devraient correspondre. Néanmoins, l'article 3 de l'accord prévoit que les compagnies aériennes peuvent transférer des données au-delà des dix-neuf éléments de données de dossiers passagers requis. Toutefois, cette disposition soumet le DHS à l'obligation de supprimer ces données dès réception, car ce dernier n'est pas autorisé à les utiliser.

⁴⁴⁷ Accord PNR, article 3.

⁴⁴⁸ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

⁴⁴⁹ Accord PNR, annexe.

⁴⁵⁰ Guidelines on Passenger Name Record (PNR) Data, Doc 9944, OACI.

⁴⁵¹ Ibidem

⁴⁵² PNRGOV est une norme de dossiers passagers mise en place par l'UE en 2016.

Le DHS américain⁴⁵³ se trouve devant un format dans lequel les données PNR collectées doivent relever des catégories que la loi a fixées mais sans réellement de garde-fous qui permettent de se prémunir d'abus. Se pose ici le problème des règles encadrant la collecte des données personnelles des passagers aériens. En effet, les compagnies aériennes doivent collecter les données conformément aux règles des pays dans lesquels ils sont basés. Or, l'accord ne traite pas de cette question ; tout au plus, il mentionne que « les transporteurs doivent fournir les données PNR contenues dans leurs systèmes de réservation ». Conséquemment, ces données personnelles sont laissées à la merci des transporteurs aériens, sans explication de la manière de protéger ces données dans la pratique.

Le renvoi aux « normes DHS » ne fait que confirmer l'emprise exclusive et sans contrepartie des autorités américaines sur l'utilisation, la collecte et le transfert de ces données personnelles ; des normes qui diffèrent des normes européennes. Par ailleurs, le citoyen européen n'est pas à même de juger des standards de protection qu'offrent ces « normes DHS ». Certains éléments de données des dossiers peuvent être facilement compris par le citoyen européen comme le nom du passager, la date du voyage et la date de la réservation.

Toutefois, d'autres éléments de données nécessitent une certaine expertise dans le domaine. C'est le cas, par exemple, de la catégorie des données relatives aux informations de paiement⁴⁵⁴ qui doivent être transférées aux États-Unis. En effet, dans le cas où le paiement n'est pas effectué par le passager, des données personnelles appartenant à un tiers qui effectue le paiement, tel que l'employeur du passager, peuvent être concernées. Cela met en jeu les données personnelles d'un individu qui n'est ni informé de ces opérations ni à même de comprendre les enjeux de ces transferts et qui, d'ailleurs, n'a pas donné son consentement à cette opération. Ce vide juridique montre les limites de cet accord, dévoilant ainsi une exposition des citoyens européens à une situation juridique⁴⁵⁵ dans laquelle ils n'ont plus d'emprise sur leurs droits.

Une autre catégorie de données à caractère personnel peut faire l'objet de contentieux. Les données liées aux remarques générales sur les passagers, telles que les OSI (Other Service Information), SSI (Special Service Information) et SSR (Special Service Request), peuvent

⁴⁵³ D. VAN PUYVELDE, « Sécurité de l'information et partenariats public-privé dans le renseignement américain », *Sécurité et stratégie*, 2014, pp. 25-30 en ligne à URL : <https://www.cairn.info/revue-securite-et-strategie-2014-2-page-25.htm> consulté le 3 octobre 2023.

⁴⁵⁴ J.-C. PAILLÈS, « Les systèmes de paiement électronique sur internet », *Les cahiers du numérique*, 2003, pp. 45-69. L'auteur note à quel point ce paiement est devenu un acte banal auquel le consommateur ne prête plus attention.

⁴⁵⁵ L. FARET, « Enjeux migratoires et nouvelle géopolitique à l'interface Amérique latine-États-Unis », *Hérodote*, 2018, pp. 48-105.

inclure des informations personnelles sensibles, comme les croyances religieuses (par exemple, les préférences alimentaires) ou l'état de santé (par exemple, les demandes de fauteuil roulant)⁴⁵⁶. Ces données sont susceptibles d'être considérées comme sensibles, et leur traitement peut être, en principe, interdit par le droit européen⁴⁵⁷. En effet, l'article 9 du RGPD qualifie de sensibles les données qui révèlent des informations telles que l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données génétiques, biométriques, et celles relatives à la santé, à la vie sexuelle ou à l'orientation sexuelle. En principe, leur traitement est interdit.

Toutefois, le deuxième paragraphe de l'article 9 énumère les exceptions à cette interdiction⁴⁵⁸. Parmi celles-ci, figurent les cas où la personne concernée a donné son consentement explicite, ou lorsque le traitement est nécessaire pour remplir des obligations légales, sauvegarder des intérêts vitaux, ou exercer des droits en matière de droit du travail, de sécurité sociale ou de protection sociale.

De plus, certaines organisations à but non lucratif poursuivant des finalités politiques, philosophiques, religieuses ou syndicales peuvent également traiter ces données dans le cadre de leurs activités légitimes, sous réserve de garanties appropriées et de la non-communication des données en dehors de l'organisme sans consentement. Le traitement est aussi permis pour des raisons d'intérêt public, notamment dans les domaines de la santé publique, de la recherche scientifique, ou de la justice.

L'article 6 de l'accord PNR euro-américain reconnaît la présence de données sensibles dans les dossiers passagers et prévoit l'utilisation de systèmes automatisés pour filtrer et masquer ces données⁴⁵⁹. Le DHS est tenu de fournir à la Commission européenne, dans un délai de 90 jours à compter de l'entrée en vigueur de l'accord, une liste de codes et de termes permettant d'identifier les données sensibles qui seront filtrées⁴⁶⁰.

En principe, le DHS ne doit pas traiter ni utiliser ces données, sauf dans des circonstances exceptionnelles⁴⁶¹. Dans ces circonstances exceptionnelles, lorsque la vie d'une personne

⁴⁵⁶ E. E. ANDERSON, J. CHOUBINEH, « Enterprise information security strategies », *Computers & Security*, Vol. 27, p. 23, 2008 ; W. H. Ware, « Security Controls for Computer Systems : Report of Defense Science Board Task Force on Computer Security », *RAND Report R-609-1*, p. xi, octobre 1979.

⁴⁵⁷ Article 9, 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, RGPD).

⁴⁵⁸ RGPD, article 9, paragraphe 2.

⁴⁵⁹ Accord PNR, article 6 (1).

⁴⁶⁰ Accord PNR, article 6 (2).

⁴⁶¹ Accord PNR, article 6 (3).

pourrait être menacée ou gravement en péril, l'accès aux données sensibles et leur utilisation sont autorisés. Cet accès est strictement encadré par des procédures restrictives au cas par cas et nécessite l'accord d'un responsable de haut niveau du DHS.

Les données sensibles doivent être effacées définitivement au plus tard 30 jours après la dernière réception du dossier passager contenant ces données. Toutefois, elles peuvent être conservées pour une durée plus longue, précisée dans la législation des États-Unis, mais uniquement aux fins d'enquêtes, de poursuites ou de mesures répressives spécifiques, conformément aux lois américaines en vigueur⁴⁶².

Contrairement aux règles de conservation, l'accord PNR reste vague sur les modalités de consultation des données sensibles. Il ne précise pas si les limitations mentionnées s'appliquent également à l'utilisation de ces données « aux fins d'enquêtes, de poursuites ou de mesures répressives spécifiques ». Ce flou juridique renforce l'avantage accordé aux autorités américaines, en leur offrant une plus grande flexibilité dans l'exploitation des dossiers passagers, et souligne la prédominance d'une approche sécuritaire au détriment de la protection des données sensibles⁴⁶³.

Section 2 - La présence de la logique répressive américaine dans la directive européenne sur les dossiers passagers

La politique pénale aux États-Unis⁴⁶⁴ du début du XXI^e siècle est caractérisée par une logique violemment répressive et se traduit par un taux d'incarcération le plus élevé au monde, soit 639 détenus par tranche de 100 000 habitants, loin devant le Brésil (357) et très loin devant les Pays-Bas (63) ou l'Inde (35) » selon le classement du World Prison Brief et de l'Institute for Crime & Justice Policy Research (ICPR)⁴⁶⁵, avec près de 11 millions de citoyens en prison ou en maison d'arrêt en 2021.

Ce constat est le résultat d'un politique qui a commencé à être mise en œuvre quelques décennies auparavant. Dans les années 1980, les candidats républicains et démocrates se sont engagés dans une surenchère de mesures punitives (*tough on crime laws*). Citons aussi

⁴⁶² Accord PNR, article 6 (4).

⁴⁶³ A. TÜRK, P. PIAZZA, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée, Entretien avec Alex TÜRK ; propos recueillis par Pierre PIAZZA », *Cultures & Conflits*, 2004, pp. 115-134.

⁴⁶⁴ E. HINTON, *From The War On Poverty To The War On Crime: The Making Of Mass Incarceration in America*, Cambridge, Harvard University Press, 2016. Voir M. VEAUDOR, « Politique pénale et préjugé racial aux États-Unis », La vie des idées, 6 mars 2016, en ligne à URL : https://laviedesidees.fr/IMG/pdf/20170306_massincarceration.pdf consulté le 3 octobre 2023.

⁴⁶⁵ Institute for Crime & Justice Policy Research, *Les tendances de l'incarcération*, 2021.

l'exploitation de l'affaire Willie Horton⁴⁶⁶ par le candidat G. Bush pour discréditer son adversaire M. Dukakis durant la campagne des élections présidentielles de 1988, en qualifiant sa position de « *soft on crime* » pour réduire les ambitions de son adversaire à néant. Par ailleurs, plusieurs États fédérés ont adopté une législation appliquant ladite « règle des trois coups » (*three strikes and you're out*) en référence à une règle de base-ball américain.

Ainsi, une loi a été promulguée en Californie en 1994 quelques mois après deux meurtres très médiatisés, commis par deux récidivistes, dans les affaires Kimberley Reynolds (1992) et de Polly Klaas (1993). Cette législation impose au juge de doubler la peine de tout individu préalablement condamné pour une atteinte aux personnes, lorsque le récidiviste est reconnu coupable d'un nouveau crime (*felony*) commis contre une personne (*violent crime*) ou contre un bien (*property crime*). Cette règle-loi prévoit également que toute personne préalablement condamnée à deux reprises pour atteinte aux personnes reçoit automatiquement une peine de vingt-cinq ans de prison si elle est de nouveau reconnue coupable d'une atteinte aux personnes ou aux biens et sans délai de prescription⁴⁶⁷.

Puis, la réaction des autorités américaines aux attentats terroristes du 11 septembre 2001 a été le catalyseur d'un droit répressif⁴⁶⁸ supranational, autrement dit allant au-delà du territoire américain, et touchant l'utilisation des données personnelles des passagers aériens. Ce nouveau droit dépasse les frontières des États-Unis et a influencé le droit européen comme on peut le constater à la lecture de la directive relative à la prévention et la détection des infractions terroristes et formes graves de criminalité via le transfert des données passagers par les transporteurs aériens et leur traitement, en date du 27 avril 2016 (sous-section 1). Or, la priorité donnée à l'utilisation des dossiers passagers dans la lutte contre le terrorisme et les formes de graves de criminalité créé un déséquilibre entre la sécurité collective et la protection des droits fondamentaux pourtant traditionnellement protégées par l'Union européenne, en fragilisant le droit à la vie privée et la protection des données personnelles des passagers aériens (sous-section 2).

⁴⁶⁶ William Horton est un criminel noir condamné à perpétuité dans le Massachusetts, alors gouverné par Michael Dukakis. En 1987, il avait profité d'une sortie provisoire dans le cadre d'un programme de réinsertion pour commettre une agression et un viol. George Bush exploita l'affaire dans ses discours et spots télévisés, au cours de la campagne présidentielle de 1988, pour dénoncer le supposé laxisme de son adversaire démocrate en matière de lutte contre la criminalité.

⁴⁶⁷ F. VINDEVOGEL, « La remise en question des politiques pénales ultra-répressives : tendance lourde ou évolution conjoncturelle ? », *Revue française d'études américaines*, 2007/3 (n° 113), pp. 92-107, 2007.

⁴⁶⁸ F. CHALTIEL, « Le Traité de Lisbonne : la réforme du système contentieux européen - L'État de droit européen renforcé », *Petites affiches*, Lextenso, 2008. Voir aussi M.-A. COHENDET, « Le droit répressif, quelles valeurs, quelles frontières ? », *Revue juridique de l'environnement*, 2014, pp. 15-32.

Sous-section 1 – Une directive européenne reprenant la préoccupation américaine vis-à-vis des infractions terroristes

La directive européenne PNR vise à réglementer le transfert des données des passagers aériens par les compagnies aériennes aux autorités nationales. Avec la collecte des données de passagers aériens, les autorités compétentes peuvent confronter les données de passagers à diverses bases de données de personnes recherchées.

§ 1 – Un PNR européen basé sur la coopération mais sous influence américaine

Comme le souligne Vincent Correia, l'idée de mise en place d'un PNR dans l'espace européen est fortement influencée par le modèle américain⁴⁶⁹. Historiquement, elle apparaît d'abord avec la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs aériens de communiquer les données relatives aux passagers, régissant le transfert préalable aux autorités compétentes en vue d'améliorer les contrôles aux frontières et de lutter contre l'immigration clandestine. L'objet du texte est moins étendu qu'un PNR puisqu'il ne couvrirait pas la lutte contre les infractions terroristes ni le crime organisé. Par ailleurs, la directive a été transposée de manière inégale par les États membres⁴⁷⁰.

Puis, le 6 novembre 2007, la Commission européenne a adopté une proposition de décision-cadre du Conseil relative à l'utilisation des données personnelles des dossiers passagers à des fins répressives⁴⁷¹. Toutefois, n'ayant pas encore été adoptée par le Conseil lors de l'entrée en vigueur du Traité de Lisbonne le 1^{er} décembre 2009, la proposition a été ignorée. Un nouveau projet a été conçu en 2011 dont les négociations ont abouti à une directive en 2016.

En effet, le 27 avril 2016, le Parlement européen et le Conseil ont adopté une directive relative à la prévention et la détection des infractions terroristes et formes graves de criminalité à l'aide du transfert des données passagers et leur traitement par les transporteurs aériens⁴⁷². Cette directive européenne a plusieurs objectifs. Tout d'abord, elle vise à la mise en place d'une coopération entre États membres, permettant l'échange et l'exploitation de données PNR, tout en respectant les libertés publiques ; ensuite, elle favorise les conditions d'un début de coordination entre les fichiers de dossiers passagers des États membres ; enfin, elle vise à ce que les États membres créent un cadre juridique régissant les obligations des

⁴⁶⁹ V. CORREIA, *L'Union européenne et le droit international de l'aviation civile*, Bruylant, 2014, pp. 646-647.

⁴⁷⁰ Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.

⁴⁷¹ Commission européenne, Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives, COM(2007) 654 final, 6 novembre 2007.

⁴⁷² 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.

transporteurs aériens en matière de transmission des données de dossiers passagers et les modalités communes de traitement.

L'intitulé de cette directive montre un léger décalage entre les conceptions européenne et américaine vis-à-vis du PNR. En effet, tandis que l'accord euro-américain, rédigé sous la pression américaine, vise à « combattre efficacement le terrorisme » et « les formes graves de criminalité transnationale », la directive européenne évite le concept américain, notamment du Président George W. Bush, de « guerre contre le terrorisme »⁴⁷³, en parlant « d'infractions terroristes » et « de formes graves de criminalité » au lieu de « criminalité internationale ». Cette terminologie différente semble, *a priori*, traduire une conception distincte du rôle que doivent jouer les dossiers passagers, qui se distingue nettement de l'approche américaine.

Or, le cinquième considérant de la directive vient rappeler l'utilisation des dossiers passagers pour un objectif avant tout répressif⁴⁷⁴. Il énonce en effet que : « Les objectifs de la présente directive sont, entre autres, d'assurer la sécurité, de protéger la vie et la sécurité des personnes, et de créer un cadre juridique pour la protection des données PNR en ce qui concerne leur traitement par les autorités compétentes »⁴⁷⁵. La protection des données PNR vient donc en dernière place des objectifs énoncés, devancée par l'élément sécuritaire. Certes, ce considérant se veut équilibré dans sa conception de l'utilisation des dossiers passagers, toutefois les rédacteurs ont clairement montré que la priorité est accordée à une conception sécuritaire de l'utilisation des données personnelles des passagers aériens.

Les considérants six et sept de la directive confirment l'approche sécuritaire sous-tendant l'usage des données personnelles des passagers aériens en énonçant que « l'utilisation effective des données PNR, par exemple la confrontation des données PNR à diverses bases de données de personnes ou d'objets recherchés, est nécessaire 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 donc pour renforcer la sécurité intérieure, pour rassembler des preuves et, le cas échéant, pour trouver les complices de criminels et démanteler des réseaux criminels »⁴⁷⁶.

⁴⁷³ C. BUNZEL, "Jihadism on its own terms", *Hoover Institution Press*, 2017.

⁴⁷⁴ Y. MAYAUD, *Terrorisme*, Dalloz, 2021. Voir aussi R. PARIZOT, « Surveiller et prévenir... à quel prix ? Loi n°2015-912 du 24 juillet 2015 relative au renseignement », *La semaine juridique*, LexisNexis, 2015.

⁴⁷⁵ Considérant 5), Directive (UE) 2016/681 du Parlement européen et du Conseil, du 27 avril 2016, relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

⁴⁷⁶ Considérant 6, Ibidem

Le considérant permet de justifier la nécessité de l'utilisation du PNR tandis que le septième considérant, tout en rappelant que « l'utilisation des données PNR permet de contrer la menace que représentent les infractions terroristes et les formes graves de criminalité sous un angle autre que par le traitement d'autres catégories de données à caractère personnel »⁴⁷⁷, se veut rassurant en affirmant que « l'évaluation des données PNR permet d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité avant cette évaluation et qui devraient être soumises à un examen plus approfondi par les autorités compétentes » et en précisant que « la création et l'application de critères d'évaluation devraient être limitées aux infractions terroristes et aux formes graves de criminalité pour lesquelles l'utilisation de tels critères est pertinente. Par ailleurs, les critères d'évaluation devraient être définis d'une manière qui réduise au minimum le nombre d'identifications erronées de personnes innocentes par le système ». La confirmation de l'utilisation des données PNR à des fins répressives par la directive se veut tempérée par des critères d'évaluation⁴⁷⁸ qui devraient empêcher que des personnes innocentes soient lésées.

§ 2 – La confirmation de règles communes d'accès aux données personnelles des dossiers passagers

La directive sur les données PNR édicte des règles communes d'accès aux données. En ce qui concerne leur transfert⁴⁷⁹, le texte prévoit le transfert de données des passagers de vols internationaux ainsi que le traitement de données, comme la collecte, ainsi que l'échange de ces données entre autorités étatiques (article 1). La directive est applicable aux vols intra-UE lorsque les États membres en font la demande (article 2). Les pays de l'Union européenne peuvent également choisir de collecter et de traiter les données PNR d'opérateurs économiques autres que les transporteurs aériens tels que les agences et organisateurs de voyages. Le contexte de menaces terroristes devrait logiquement inciter les États membres à faire usage de ces dispositions⁴⁸⁰.

⁴⁷⁷ Considérant 7, Ibid.

⁴⁷⁸ O. H. GANDY, « Data mining, surveillance, and discrimination in the post-9/11 environment », in Haggerty K., Ericson R. (Eds.), *The new politics of surveillance and visibility*, University of Toronto Press, 2006, pp. 363-384.

⁴⁷⁹ D. KORFF, M. GEORGES, "Passenger Name Records, data mining & data protection: the need for strong safeguards", *The Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data*, 2015, p. 34. Voir aussi M. RICH, « Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment », *University of Pennsylvania Law Review*, 2016, en ligne à URL : <http://ssrn.com/abstract=2593795> consulté le 20 octobre 2023.

⁴⁸⁰ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.

La directive appelle également les États membres à créer des Unités Information Passagers (UIP). En France, celles-ci ont été instituées dès 2014. En outre, son article 4 permet un possible échange entre les différents UIP des États membres. À la tête de chaque unité est nommé un délégué à la protection des données (DPO). Par ailleurs, les États membres ont la faculté d'échanger, entre eux et avec Europol, les données PNR qu'ils reçoivent aux fins de prévention et de détection des infractions terroristes (article 10)⁴⁸¹.

Pour le traitement des données personnelles des passagers aériens, le législateur européen a choisi la méthode « push » qui implique que les transporteurs aériens les transmettent à l'autorité requérante, ce qui permet aux premiers de garder le contrôle sur les données transmises (article 6). Cette méthode est réputée offrir un niveau plus élevé de protection des données personnelles dans la mesure où les États membres ne disposent pas d'un accès direct aux systèmes informatiques des transporteurs. L'utilisation de cette méthode est obligatoire et il appartient à l'IUP de l'État membre qui reçoit ces informations de traiter ces données. Par ailleurs, les pouvoirs de cet organisme sont strictement encadrés ; il ne peut les traiter que pour des finalités à caractère répressif.

Les données PNR sont utilisées de deux manières⁴⁸². Le premier, le mode réactif, part du principe qu'après la commission de l'infraction, les PNR vont aider les services en charge de la sécurité publique à prévenir et à détecter d'autres infractions graves, dont le terrorisme, à enquêter sur celles-ci et à poursuivre leurs auteurs. Lorsque cela est fait en temps réel, les données PNR permettent d'identifier des personnes auparavant « inconnues » des autorités qui n'étaient pas soupçonnées de participation à une infraction grave ou à un acte de terrorisme mais dont l'analyse des données indique qu'elles peuvent être impliquées dans une infraction de cette nature et qu'elles devraient donc être soumises à un examen approfondi par les autorités compétentes. La seconde manière, en temps réel, permet d'identifier les personnes dont les données de déplacement sont suspectes comme les ressortissants européens soupçonnés de vouloir rejoindre les mouvements djihadistes au Proche-Orient, en Afrique ou en Asie centrale⁴⁸³. Enfin, il est requis de la part des États membres d'arrêter une liste des

⁴⁸¹ Ibidem.

⁴⁸² R. BELLANOVA, D. DUEZ, « Le citoyen face aux nouvelles pratiques sécuritaires de l'Union européenne : enjeux démocratiques d'une sécurité par les fichiers », *Espace populations sociétés*, 2012/3, 2012, pp.49-62, en ligne à URL : <http://journals.openedition.org/eps/5104> consulté le 20 octobre 2023. Voir également A. DAUCHY, « Dreaming biometrics in Niger: The security techniques of migration control in West Africa », *Security Dialogue*, 2023.

⁴⁸³ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

autorités habilitées à travailler avec les UIP. Cette disposition permet de disposer d'une traçabilité⁴⁸⁴ des personnes et entités qui ont eu à traiter ces données PNR.

En France, par exemple, le législateur a mis en place un régime de collecte des données des dossiers passagers dès 2014. Créé à titre expérimental jusqu'au 31 décembre 2017, ce dernier répondait aux besoins de la « prévention et de la constatation des actes terroristes, des infractions mentionnées à l'article 695-23 du Code de procédure pénale et des atteintes aux intérêts fondamentaux de la Nation, du rassemblement des preuves de ces infractions et de ces atteintes ainsi que de la recherche de leurs auteurs ». Les dispositions du Code de la sécurité intérieure⁴⁸⁵ définissaient le contenu et les conditions d'exploitation du nouveau fichier national de données des passagers (système API-PNR France). Le système a été reconduit à l'issue de la phase d'expérimentation.

Précisément, le décret n° 2014-1095 du 26 septembre 2014 a créé un traitement de données à caractère personnel dénommé « système API-PNR France » pris par application de l'article 232-7 du Code de la sécurité intérieure. De plus, le décret n° 2014-1566 du 22 décembre 2014 a permis la création d'un service à compétence nationale dénommé « Unité Information Passagers » (UIP) préconisée par une directive européenne, comme nous l'avons déjà relevé. Cette dernière est un service à compétence nationale rattaché au ministre chargé des douanes dont la mission est de gérer le système API-PNR France et de répondre aux requêtes des services de sécurité ayant accès à la plateforme. Elle a surtout pour objet de récupérer et de rapprocher ces données avec le fichier des personnes recherchées, notamment pour leur implication dans des actes de terrorisme.

L'objectif de ce système est de recueillir toutes les données API-PNR des 230 compagnies françaises et étrangères desservant le territoire national, à l'exclusion des vols intérieurs, soit l'équivalent de 200 millions de dossiers par an⁴⁸⁶. Les données PNR sont davantage utilisées en tant qu'outil de renseignement en matière criminelle et instrument de contrôle aux frontières. Elles doivent permettre une coopération accrue entre les services répressifs pour lutter contre les formes les plus graves de criminalité. Ce texte confirme l'influence de la vision américaine en matière de règles relatives à l'utilisation des dossiers passagers⁴⁸⁷.

⁴⁸⁴ V. GAUTRON, D. MONNIAUX, « De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme », *Archives de politique criminelle*, 2016, pp. 123-135.

⁴⁸⁵ Article R. 232-12 du Code de la sécurité intérieure.

⁴⁸⁶ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

⁴⁸⁷ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.

L'efficacité du PNR dans la lutte contre le crime organisé s'explique par le fait que les données fournies par les transporteurs aériens aux autorités répressives sont disponibles en amont des déplacements⁴⁸⁸. Ainsi, le traitement de ces données personnelles des passagers aériens permet une intervention efficace contre les auteurs d'infractions. À titre d'illustration, l'analyse de l'utilisation du PNR par la cellule de ciblage de Roissy montre que 80% des saisies de cocaïne ont été réalisées grâce à l'utilisation du PNR⁴⁸⁹. Le taux de réussite des constatations obtenues grâce à un ciblage au moyen des données PNR est 7 fois supérieur à celui obtenu par d'autres méthodes d'analyse. En effet, les douanes françaises, s'appuyant sur l'article 65 du code des douanes, peuvent demander aux compagnies aériennes de leur transmettre des données PNR.

Sous-section 2 – Une directive européenne reléguant la protection des droits fondamentaux

La directive européenne 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers produit des effets, non sans conséquences, sur la vie privée et la protection des données personnelles des passagers aériens.

§ 1 – Une directive européenne fragilisant la vie privée des passagers aériens

Dès l'adoption par la Commission européenne, en novembre 2007, d'un projet-cadre de directive sur l'utilisation des données des dossiers passagers, le G29⁴⁹⁰ a relevé l'absence de garanties permettant d'assurer la protection des données personnelles des passagers aériens quant à leur vie privée⁴⁹¹. Les travaux des institutions européennes ont conduit à une amélioration du texte initial sur ce point, ce qui a permis l'adhésion progressive du Parlement européen à un projet considéré par ses détracteurs comme liberticide⁴⁹². En effet, la Commission des transports et du tourisme a, par exemple, considéré « qu'il convient de renforcer les droits des passagers à la confidentialité et à la sécurité des données, ainsi que leurs droits d'accès, de rectification, d'effacement et de blocage des données, de même qu'en

⁴⁸⁸ Ibidem.

⁴⁸⁹ Ibid.

⁴⁹⁰ Organe indépendant et consultatif, le groupe de travail « article 29 » sur la protection des données a été institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

⁴⁹¹ G29, Avis commun sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR), à des fins répressives, présentée par la Commission le 6 novembre 2007.

⁴⁹² Parlement européen, deuxième rapport sur la proposition de directive du Parlement européen et du Conseil, op. cit., 7 septembre 2015, avis de la Commission des affaires étrangères et de la Commission des transports et du tourisme, pp. 68-69 et 116-118.

matière d'indemnisation et de recours juridictionnel. En particulier, il importe d'améliorer le droit d'accès que la décision-cadre limite fortement »⁴⁹³.

L'opinion des détracteurs du projet se basait sur l'idée selon laquelle les PNR seraient des « filets dérivants » à même de capturer des données personnelles de passagers aériens afin de détecter des activités terroristes ou criminelles tout en étant en mesure d'utiliser ces données après plusieurs années⁴⁹⁴. En principe, les États membres interdisent le traitement des dossiers passagers qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle (article 13.4)⁴⁹⁵. Dans le cas où l'UIP d'un État membre collecterait de telles données, il est appelé à les effacer immédiatement.

Listés à l'annexe 1 de la directive⁴⁹⁶, les dossiers passagers contiennent les données personnelles suivantes : le code repère du dossier passager, la date de réservation et/ou d'émission du billet, les dates prévues du voyage, les noms, l'adresse et les coordonnées (numéro de téléphone, adresse électronique), toutes les informations relatives aux modes de paiement, y compris l'adresse de facturation, l'itinéraire complet pour le PNR concerné, les informations « grands voyageurs », l'agence de voyages et/ou l'agent de voyages, le statut du voyageur, y compris les confirmations, l'enregistrement, la non-présentation ou un passager de dernière minute sans réservation, les indications concernant la scission ou la division du PNR, les remarques générales (notamment toutes les informations disponibles sur les mineurs non accompagnés de moins de 18 ans, telles que le nom et le sexe du mineur, son âge, la ou les langues parlées, le nom et les coordonnées du tuteur présent au départ et son lien avec le mineur, le nom et les coordonnées du tuteur présent à l'arrivée et son lien avec le mineur, l'agent présent au départ et à l'arrivée), les informations sur l'établissement des billets, y compris le numéro du billet, la date d'émission, les allers simples, les champs de billets informatisés relatifs à leur prix, le numéro du siège et autres informations concernant le siège, les informations sur le partage de code, toutes les informations relatives aux bagages, le nombre et autres noms de voyageurs figurant dans le PNR, toute information préalable sur les

⁴⁹³ Ibidem

⁴⁹⁴ Y. DETRAIGNE, Rapport n°441, fait au nom de la Commission des Lois constitutionnelles, de législation sur la proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives, 13 mai 2009.

⁴⁹⁵ Le droit européen place la personne concernée au centre de l'utilisation de ses données. Voir en ce sens E. DEBIES, « Renforcement des droits des individus sur leurs données personnelles : quelles conséquences sur l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) ? », *Regards*, 2019, pp. 149-155.

⁴⁹⁶ Annexe 1, 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.

passagers (données API) qui a été recueillie (y compris le type, le numéro, le pays de délivrance et la date d'expiration de tout document d'identité, la nationalité, le nom de famille, le prénom, le sexe, la date de naissance, la compagnie aérienne, le numéro de vol, la date de départ, la date d'arrivée, l'aéroport de départ, l'aéroport d'arrivée, l'heure de départ et l'heure d'arrivée) et l'historique complet des modifications des données PNR énumérées aux points 1 à 18.

Pascal Dupont considère que ces 19 catégories de données personnelles de passagers aériens prévues par la directive pour permettre de tracer un passager aérien au cours de ses déplacements ne concernent que les caractéristiques du vol sans avoir d'impact sur la vie privée. Il ne s'agirait donc pas d'une collecte massive et indiscriminée de données personnelles⁴⁹⁷.

Selon la directive européenne, les données liées aux remarques générales sur le passager, tels que les OSI (Other Service Related Information), SSI (Special Service Information) et SSR (Special Service Request) pouvant révéler des données personnelles liées aux croyances religieuses ou à la santé, de nature sensible, ne sont pas incluses dans les catégories recueillies par les transporteurs aériens. Toutefois, l'hypothèse, du moins technique, que les transporteurs aériens recueillent ces données, existe bien. Par conséquent, la fragilité, en pratique, de la protection de la vie privée des passagers aériens n'est pas écartée.

§ 2 – Une directive européenne fragilisant la protection des données personnelles des passagers aériens

La garantie de protection des données personnelles par la directive européenne a soulevé quelques controverses⁴⁹⁸, souvent relancées, entre les défenseurs de la sécurité collective et ceux des droits fondamentaux ; cela a été le cas lorsque des attentats ont été commis sur le sol européen entre 2010 et 2020⁴⁹⁹. Ces débats intervenaient dans un contexte géopolitique délicat caractérisé par des conflits en Syrie et en Irak attirant des combattants étrangers qui ont ensuite pris le chemin vers les capitales européennes⁵⁰⁰ après la défaite de l'État islamique en Irak et au Levant (EI). En droit européen, la protection des données à caractère personnel est

⁴⁹⁷ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

⁴⁹⁸ G-29, Avis commun à la proposition de décision cadre du Conseil relative à l'utilisation des PNR à des fins répressives, le 6 novembre 2007, 02/22/07/EU.

⁴⁹⁹ O. KEMPF, « Les combattants étrangers jihadistes, entre modernisme et mutation », *Revue Défense Nationale*, 2015, pp. 111-116. Voir aussi Rédaction, « Attentats: qu'est-ce que le PNR, ce fichier européen qui fait tant polémique ? », *L'Express*, 23 mars 2016.

⁵⁰⁰ A. CEYHAN, « Les technologies européennes de contrôle de l'immigration, vers une gestion électronique des 'personnes à risque' », *Réseaux*, 2010, pp. 131-150.

énoncée par des textes majeurs. Tout d'abord, l'article 16, § 1 du Traité sur le fonctionnement de l'Union européenne (TFUE) énonce :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives 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, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes »⁵⁰¹.

Cette disposition relève des domaines de la coopération judiciaire en matière pénale et de la coopération policière. Elle couvre le traitement transfrontalier et national des données à caractère personnel.

En revanche, l'article 16, § 2 du TFUE renvoie à l'article 39 du Traité de l'Union européenne (TUE) qui précise que le Conseil adopte, seul, les décisions fixant les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ de la politique étrangère et de la sécurité commune⁵⁰². Sous ces réserves, l'article 87, § 2 du TFUE indique qu'en vue de développer « une coopération policière qui associe toutes les autorités compétentes des États membres, y compris les services de police, les services des douanes et autres services répressifs spécialisés dans les domaines de la prévention ou de la détection des infractions pénales et des enquêtes en la matière », le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, peuvent établir des « mesures portant sur la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes »⁵⁰³.

Toutefois, certaines précautions ont été intégrées, comme l'illustre la déclaration 21 relative à la protection des données personnelles dans le cadre de la coopération judiciaire en matière pénale et de la coopération policière. Cette déclaration, annexée à l'acte final de la conférence intergouvernementale ayant adopté le Traité de Lisbonne et au TFUE, souligne que des règles spécifiques, fondées sur l'article 16 du TFUE, pourraient être nécessaires pour la protection

⁵⁰¹ Article 16, § 1, Traité sur le fonctionnement de l'Union européenne.

⁵⁰² Article 16, § 2, Traité sur le fonctionnement de l'Union européenne.

⁵⁰³ Article 87, § 2, Traité sur le fonctionnement de l'Union européenne.

des données personnelles et leur libre circulation dans ces domaines, en raison de la nature particulière des activités concernées⁵⁰⁴.

L'article 8 de la Charte des droits fondamentaux de l'Union européenne reconnaît la protection des données à caractère personnel comme un droit fondamental⁵⁰⁵. Il stipule que chaque individu a droit à la protection de ses données personnelles, lesquelles doivent être traitées de manière loyale, à des fins spécifiques, et sur la base du consentement de la personne concernée ou d'un autre fondement légitime prévu par la loi. En outre, chaque personne a le droit d'accéder aux données la concernant et de demander leur rectification. Le respect de ces règles est assuré par une autorité indépendante.

L'article 52 de la Charte prévoit la possibilité de restreindre l'exercice des droits et libertés qu'elle garantit, à condition que ces restrictions soient prévues par la loi et qu'elles respectent « l'essence même de ces droits et libertés »⁵⁰⁶. Conformément au principe de proportionnalité, de telles limitations ne peuvent être imposées que si elles sont nécessaires et qu'elles répondent véritablement à des objectifs d'intérêt général reconnus par l'Union ou à la nécessité de protéger les droits et libertés d'autrui.

Au cours des travaux d'élaboration de la directive européenne, le contrôleur européen de la protection des données a rappelé que le respect des principes de nécessité et de proportionnalité figurait parmi les conditions préalables essentielles à la mise en place d'un PNR européen⁵⁰⁷. La Commission des libertés civiles du Parlement européen, qui avait rejeté en 2013 le projet de texte au motif que les droits individuels n'étaient pas suffisamment garantis⁵⁰⁸, a donné son feu vert à une version améliorée en décembre 2015⁵⁰⁹. Le vote du 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

⁵⁰⁴ Anand Menon mentionne l'opinion partagée par une communauté d'observateurs selon laquelle l'objectif prioritaire du Traité de Lisbonne est de donner une sécurité plus efficace à l'Union européenne. A. MENON, « La politique de défense européenne après le traité de Lisbonne, beaucoup de bruit pour rien », *Politique étrangère*, 2011, pp. 375-387. Voir aussi J. MONAR, « La mise en œuvre de l'espace de liberté, de sécurité et de justice : un défi pour l'Union européenne et pour les États membres », *Revue française d'administration publique*, 2009, pp. 15-34.

⁵⁰⁵ Charte des droits fondamentaux de l'Union européenne, article 8.

⁵⁰⁶ Charte des droits fondamentaux de l'Union européenne, article 25.

⁵⁰⁷ Communiqué de presse, « Données PNR de l'UE : le CEPD met en garde contre une collecte massive et indue des données des passagers », *EDPS*, EDPS/2015/085, septembre 2015.

⁵⁰⁸ Les eurodéputés avaient voté le 24 avril 2013 en majorité contre la proposition de directive PNR dénonçant l'absence de garanties concernant la proportionnalité du traitement des données des passagers et la nécessité du transfert.

⁵⁰⁹ Parlement européen, Proposition sur les données des dossiers passagers de l'UE, 4 décembre 2015.

et à la libre circulation de ces données⁵¹⁰, abrogeant la directive 95/46/CE, a satisfait les eurodéputés hostiles au projet PNR. Ceci renforça le cadre législatif européen jugé fragile⁵¹¹.

Les partisans de la directive PNR, tels que Pascal Dupont⁵¹², soulignent que l'article 13 de la directive offre plusieurs garanties pour protéger les données personnelles des passagers, notamment les droits d'accès, de rectification, d'effacement, et de limitation, ainsi que des recours juridiques. La directive impose aux États membres de veiller à ce que les données soient collectées uniquement pour des finalités déterminées, explicites et légales, et que leur traitement soit strictement limité à ces finalités. La décision-cadre 2008/977/JAI⁵¹³, qui encadre cette directive, définit également les concepts clés liés aux données personnelles et à leur traitement.

§ 3 – Une directive européenne encadrée par la jurisprudence de la CJUE

Le 21 juin 2022, les juges de Luxembourg ont rendu une décision pionnière vis-à-vis de l'encadrement de la directive PNR considérant que le respect des droits fondamentaux des passagers aériens exigeait une limitation, au strict nécessaire, des pouvoirs prévus par la directive en question. Plus précisément, la CJUE a considéré qu'en l'absence de menace terroriste actuelle et réelle ou prévisible, à laquelle doit faire face un État membre, le droit de l'Union européenne s'oppose à une législation nationale dont l'objet est « le transfert et le traitement des données PNR des vols intra-UE ainsi que des transports effectués par d'autres moyens à l'intérieur l'Union »⁵¹⁴.

En l'espèce, une association à but non lucratif, la Ligue des droits humains (LDH), avait saisi la Cour constitutionnelle belge en juillet 2017 d'un recours en annulation contre une loi du 25 décembre 2016 dont l'objet était la transposition dans l'arsenal législatif belge de la directive PNR. Selon l'association, la loi mise en cause méconnaissait le droit au respect de la vie privée et à la protection des données à caractère personnel que garantissent le droit belge et le droit de l'Union européenne. La LDH critiquait, d'une part, le contour assez large de données

⁵¹⁰ 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.

⁵¹¹ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

⁵¹² Ibidem

⁵¹³ Décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

⁵¹⁴ CJUE, « La Cour estime que le respect des droits fondamentaux exige une limitation des pouvoirs prévus par la directive PNR au strict nécessaire », *Communiqué de presse*, arrêt de la Cour dans l'affaire C-817/19, 21 juin 2022, en ligne à URL : <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105fr.pdf> consulté en ligne le 31 mars 2023.

PNR recueillis et, d'autre part, le caractère général de la collecte, du transfert et du traitement de celles-ci⁵¹⁵. Elle considérait également que la loi sur le PNR portait atteinte au principe de libre circulation des individus en ce qu'elle rétablirait indirectement des contrôles aux frontières en étendant le système PNR aux vols à l'intérieur de l'Union. En effet, l'article 2 de la directive européenne sur les dossiers passagers prévoit la possibilité pour les États membres d'appliquer ladite législation aux vols intra-UE.

En octobre 2019, la Cour constitutionnelle belge a posé dix questions préjudicielles à la CJUE portant, notamment, sur la validité de la directive européenne relative aux données des passagers aériens ainsi que sur la compatibilité de la loi belge du 25 décembre 2016 avec le droit européen. Le 21 juin 2022, la Cour a rendu son arrêt, jugeant, en premier lieu, qu'aucun élément dans la directive n'est de nature à affecter la validité de celle-ci, particulièrement au regard de son interprétation à la lumière des droits fondamentaux garantis aux articles 7 et 8 de la Charte des droits fondamentaux⁵¹⁶.

Les juges de Luxembourg ont néanmoins relevé que, malgré les références de la directive PNR à un niveau élevé de protection des données à caractère personnel conforme à la Charte des droits fondamentaux, elle comporte des atteintes significatives aux droits à la vie privée et à la protection des données. En effet, la directive instaure un régime de surveillance continue, non ciblée et systématique, incluant une évaluation automatisée des données personnelles de tous les passagers aériens⁵¹⁷.

Ce raisonnement jurisprudentiel reflète une volonté de renforcer la protection des droits fondamentaux des passagers tout en autorisant l'utilisation des données dans des cas spécifiques liés à la lutte contre le terrorisme⁵¹⁸ et la criminalité grave. La CJUE conclut que le transfert, le traitement et la conservation des données des dossiers passagers doivent être strictement limités à ce qui est nécessaire pour combattre ces infractions. Elle insiste

⁵¹⁵ Communiqué de presse, « La loi belge PNR 'Passenger Name Record' recadrée par la Cour de justice de l'Union européenne », *Ligue des droits humains*, 21 juin 2022, en ligne à URL : <https://www.liguedh.be/la-loi-belge-pnr-passenger-name-record-recadree-par-la-cour-de-justice-de-lunion-europeenne/> consulté en ligne le 31 mars 2023. Voir aussi C. VALLET, « Fichés jusqu'au ciel ? », *Alternatives internationales*, 2015, p. 19 ; E. MECHOULAN, « Faut-il créer une agence de renseignement européenne ? », *Politique étrangère*, 2019, pp. 125-139, en ligne à URL : <https://www.cairn.info/revue-politique-etrangere-2019-4-page-125.htm?ref=doi> consulté le 20 octobre 2023.

⁵¹⁶ CJUE, « La Cour estime que le respect des droits fondamentaux exige une limitation des pouvoirs prévus par la directive PNR au strict nécessaire », *Communiqué de presse*, arrêt de la Cour dans l'affaire C-817/19, 21 juin 2022, en ligne à URL : <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105fr.pdf> consulté en ligne le 31 mars 2023.

⁵¹⁷ Ibidem

⁵¹⁸ H. LABAYLE, R. MEHDI, « Terrorisme: les jours d'après », *KritV, CritQ, RCrit. Kritische Vierteljahresschrift Für Gesetzgebung Und Rechtswissenschaft, Critical Quarterly for Legislation and Law, Revue Critique Trimestrielle de Jurisprudence et de Législation*, 2015, pp. 3-7, en ligne à URL : <http://www.jstor.org/stable/43784263> consulté le 20 octobre 2023.

également sur le fait que les pouvoirs conférés par la directive PNR doivent être interprétés de manière restrictive⁵¹⁹.

⁵¹⁹ CJUE, affaire C-817/19, 21 juin 2022, en ligne à URL : <https://curia.europa.eu/juris/document/document.jsf?jsessionid=FA2FC10364C82396D18B54C13B472ABB?text=&docid=261282&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=5007600> consulté en ligne le 31 mars 2023.

TITRE 2 – L’EMPIÈTEMENT DES LÉGISLATIONS RÉPRESSIVES SUR LES DROITS FONDAMENTAUX DES PASSAGERS AÉRIENS

L’après Seconde guerre mondiale, en France comme dans la plupart des pays occidentaux, a été caractérisée par une remise en cause des finalités de la peine pénale et plusieurs discours critiques à l’égard de la prison⁵²⁰. Cette nouvelle réflexion visait à accompagner le délinquant vers un changement de comportement pour mieux l’insérer dans la société, au lieu de le châtier ou de l’éliminer. Développant un discours aux tonalités optimiste et humaniste, cette approche de la répression pénale considérait que le délinquant pouvait être réinséré moyennant une prise en charge adéquate. Dans ce contexte, le législateur a développé de nouvelles sanctions ainsi que des aménagements de peine en milieu ouvert, hors de la prison ; mentionnons la libération conditionnelle, le sursis avec mise à l’épreuve et, ultérieurement, le travail d’intérêt général. Bien qu’il ne soit pas totalement disparu, ce discours est aujourd’hui en « nette perte de vitesse » selon René Levy⁵²¹.

La tendance s’est inversée dans les pays occidentaux, notamment sous la pression des législations votées durant les mandats de Ronald Reagan et Margaret Thatcher⁵²², respectivement aux États-Unis et au Royaume-Uni, et plus tardivement ailleurs. À partir des années 1980, les législations reprennent des finalités pénales de dissuasion et de neutralisation, accompagnées d’un alourdissement des peines. En parallèle, les intérêts de la victime émergent de nouveau et tendent à prendre le dessus sur ceux du délinquant dont le crime est de moins en moins interprété comme le résultat d’un environnement socio-économique, ou un défaut de socialisation, puisque le discours juridique pointe dorénavant la responsabilité individuelle, les choix et la dangerosité objective supposée du délinquant.

Par conséquent, des peines « incompressibles »⁵²³ de condamnation à la prison, dont la durée ne peut pas être réduite, vont primer des mesures individuelles, auparavant préventives ou

⁵²⁰ R. LEVY, « Ordre social et répression pénale, Crime et insécurité : un demi-siècle de bouleversement », CNRS, 2005, en ligne à URL : <https://journals.openedition.org/sdt/20050> consulté en ligne le 31 mars 2023.

⁵²¹ Ibidem

⁵²² D. YOUNG, « Vers un nouveau droit pénal des mineurs », in *Juger et éduquer les mineurs délinquants*, Dunod, 2009, pp. 103-118. L’auteur revient sur l’impact des politiques néo-libérales qui veulent imposer une nouvelle philosophie pénale alternative dans le domaine de la criminologie rejetant le modèle thérapeutique et aspirant à imposer les thèses de l’économie de marché à l’ensemble de la société.

⁵²³ G. HOUCHON, « Les peines incompressibles », in *Pénologie, science sociale, Médecine et hygiène*, 2021, pp. 65-89. Depuis la fin des années 1980, le chercheur note que la législation pénale et l’application des sanctions

curatives⁵²⁴. En France, le nombre d'infractions enregistrées a été multiplié par huit, bien que cette croissance varie selon les types d'infractions. Dans les pays occidentaux, un mouvement général est observé dans les nouveaux domaines répressifs favorisés par des accords internationaux. Ces derniers visent à permettre aux autorités d'accéder plus rapidement aux informations concernant les individus suspectés d'activités terroristes ou liés à la criminalité organisée. Ainsi, ces accords semblent répondre aux besoins des autorités étatiques qui peinent à lutter contre une forme de criminalité qui ne connaît pas de frontières.

Les projets de textes européens peuvent mettre l'accent sur l'utilisation des données personnelles pour lutter contre le terrorisme et les crimes organisés⁵²⁵, tout en essayant de concilier ces objectifs de sécurité avec des exigences de protection des données. Cependant, ce parti pris peut avoir pour conséquence, entre autres, une protection juridique limitée des données passagers dans le cadre des accords PNR (chapitre 1).

Dans son avis 1/15, la CJUE a noté que, prises isolément, les données des dossiers passagers ne semblent pas révéler d'informations importantes sur la vie privée des personnes concernées. Cependant, lorsque ces données sont combinées, elles peuvent dévoiler un itinéraire de voyage complet, des habitudes de voyage, des relations entre plusieurs personnes, ainsi que des informations sur la situation financière des passagers, leurs habitudes alimentaires ou leur état de santé, et pourraient même fournir des informations sensibles sur ces passagers⁵²⁶.

Le raisonnement suivi par la Cour ressemble à celui adopté en matière de conservation des données des abonnés et utilisateurs des moyens de communication mobile et électronique⁵²⁷ : le seul traitement des données à caractère personnel est assimilé à une ingérence dans le droit fondamental à la vie privée⁵²⁸. Dans l'avis 1/15, les juges de Luxembourg ont souligné la possibilité de regrouper les données personnelles des passagers aériens avec d'autres bases de

dans de nombreux pays occidentaux ont été durcies dans une certaine manière, ce qui est dans une large mesure conforme à la politique pénale des États-Unis.

⁵²⁴ R. LEVY, « Ordre social et répression pénale, Crime et insécurité : un demi-siècle de bouleversement », CNRS, 2005, en ligne à URL : <https://journals.openedition.org/sdt/20050> consulté en ligne le 31 mars 2023.

⁵²⁵ M. LALDJI, « Les menaces des entités criminelles transnationales sur la sécurité intérieure des États », *Sécurité globale*, 2016, pp. 43-62. Cette priorité de lutte contre le crime organisé s'explique en partie par le fait que, comme le souligne M. Laldji, les entités criminelles transnationales ont continuellement développé leurs moyens technologiques et s'adaptent à l'évolution de leurs modes de fonctionnement. Ces groupes ne ménagent aucun effort pour exploiter les failles opérationnelles et légales, ce qui rend nécessaire une approche rigoureuse en matière de sécurité dans le transport international.

⁵²⁶ CJUE, 26 juill. 2017, avis 1/15, préc., pt. 128.

⁵²⁷ V. CORREIA, « Données des passagers aériens », *JurisClasseur Communication*, Dalloz, 15 novembre 2019.

⁵²⁸ CJUE, 8 avr. 2014, Digital Rights Ireland.

données et pointé du doigt leur analyse systématique par des moyens automatisés ou encore la durée de conservation desdites informations⁵²⁹.

Cette confrontation des régimes de collecte des données des passagers avec le droit fondamental à la vie privée n'est pas sans précédents. En effet, la Cour européenne des droits de l'Homme (CEDH), dans son arrêt *Marper*⁵³⁰, a considéré que la conservation des données personnelles constitue, par nature, une ingérence dans le droit à la vie privée. Dans sa délibération n° 2014-308 du 17 juillet 2014, la CNIL a quant à elle considéré comme dangereux le système API-PNR France en indiquant : « Eu égard à l'ampleur de ce traitement, tant au niveau du nombre de personnes concernées, du volume de données collectées, du grand nombre de personnes susceptibles d'y avoir accès, que des nouvelles conditions d'exploitation de ces données, la Commission estime que le traitement projeté est susceptible de porter une atteinte particulièrement grave au droit au respect de la vie privée et à la protection des données personnelles »⁵³¹. Des réserves similaires ont été formulées dans la déclaration du G29, à l'occasion de l'adoption de la directive (UE) 2016/681 sur la mise en place d'un système PNR européen⁵³². À cet égard, il a lieu de préciser que l'article 8 de la Charte des droits fondamentaux fait office de *lex specialis* vis-à-vis du droit à la vie privée prévu dans son article 7, érigé comme principe fondamental, dans la mesure où il est spécialement consacré à la protection des données à caractère personnel⁵³³.

Par ailleurs, les prises de position des principales institutions européennes se sont multipliées en ce sens. Ainsi, le Contrôleur européen pour la protection des données⁵³⁴, l'Agence européenne des droits fondamentaux⁵³⁵, ou encore le Groupe de l'article 29⁵³⁶ sur la protection des données ont tous émis des avis très réservés sur la proposition de décision-cadre précitée. Les critiques insistaient en particulier sur l'insuffisance d'éléments d'information et de retours d'expérience démontrant l'utilité et la nécessité de la collecte de

⁵²⁹ V. CORREIA, op. cit.

⁵³⁰ CEDH, 4 déc. 2008, n° 30562/04 et 30 566/04, *Marper c/ Royaume-Uni*.

⁵³¹ V. CORREIA, « Données des passagers aériens », *JurisClasseur Communication*, Dalloz, 15 novembre 2019.

⁵³² Ibidem

⁵³³ Ibid.

⁵³⁴ CEPD, « Avis du Contrôleur européen de la protection des données du 1er mai 2008 sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives », JOUE n° C 110, 1^{er} mai 2008.

⁵³⁵ European Union Agency for Fundamental Rights, *Twelve Operational Fundamental Rights Considerations for Law Enforcement when Processing Passenger Name Record (PNR) Data*, 13 mars 2014.

⁵³⁶ Groupe « Article 29 », Avis commun sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR), à des fins répressives, présentée par la Commission le 6 novembre 2007.

données PNR à des fins répressives⁵³⁷. Cette absence de preuve de l'intérêt du dispositif serait d'autant plus rédhibitoire que la collecte indifférenciée des données PNR de tous les passagers à destination d'un État membre de l'Union européenne est susceptible de porter une atteinte grave au respect des droits individuels⁵³⁸. Mis à part le Comité européen de la protection des données, la CJUE et, dans une moindre mesure le Parlement européen, les principales institutions européennes n'ont pas mis en avant la protection des droits fondamentaux des passagers aériens lors des négociations avec leurs homologues nord-américains (chapitre 2). À l'opposé, les services en charge de la lutte contre le terrorisme et la criminalité organisée affirment que ces données sont une mine de renseignement extrêmement utiles et que leur exploitation n'est en aucune façon redondante avec d'autres dispositifs en vigueur comme les données API ou les visas biométriques⁵³⁹. Compte tenu des retours d'expérience, les experts considèrent aussi généralement que les données PNR ne font pas double emploi avec d'autres dispositifs mais qu'elles sont plutôt une aide précieuse pour les services de sécurité⁵⁴⁰.

⁵³⁷ E. FAHEY, E. GUILD, E. KUSKONMAZ, "The novelty of EU passenger name records (PNR) in EU trade agreements: on shifting uses of data governance in light of the EU-UK trade and cooperation agreement PNR provisions", *European papers*, 2023, en ligne à URL : https://www.europeanpapers.eu/en/system/files/pdf_version/EP_eJ_2023_1_4_Articles_EFahey_EGuild_EKuskonmaz_00651.pdf consulté le 26 octobre 2023.

⁵³⁸ E. GUILD, E. BROUWER, "The political life of data: the EJC Decision on the PNR Agreement between the EU and the US", *CEPS*, 26 juillet 2006.

⁵³⁹ S. SUTOUR et Y. DETRAIGNE, « Rapport n° 401 : La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives », *Sénat*, Commission des lois, 13 mai 2009, en ligne à URL : <http://www.senat.fr/ue/pac/E6014.html> consulté en ligne le 23 mars 2023.

⁵⁴⁰ Ibidem

Chapitre 1 – Les accords PNR, un échange des dossiers passagers sans protection juridique effective

La prise en compte des droits fondamentaux, notamment ceux relatifs à la protection des données personnelles, s'est faite progressivement. Historiquement, fidèle une logique de facilitation dans la mise en place d'accords internationaux, l'annexe 9 à la Convention de Chicago⁵⁴¹ insista peu sur la protection des données des passagers, notamment au regard des actuelles exigences de protection du droit à la vie privée. Seule la pratique recommandée 9.23 semblait s'y intéresser : « Il est recommandé que les États contractants qui exigent des données PNR envisagent l'incidence de la collecte et du transfert électronique de ces données sur la confidentialité, au sein de leur propre système national, mais aussi dans les autres États. Le cas échéant, les États contractants qui exigent des données PNR et les États qui limitent l'échange de ces données devraient coopérer le plus rapidement possible pour harmoniser leurs obligations juridiques »⁵⁴².

Néanmoins, inquiétés par la relative indifférence des autorités américaines quant aux craintes suscitées par l'utilisation des données PNR, les États membres de l'Union et les institutions européennes ont progressivement insisté sur les impératifs de protection des droits fondamentaux, notamment en matière de droit à la vie privée et de droit à la protection des données. L'entrée en vigueur du Traité de Lisbonne, avec l'application de la Charte des droits fondamentaux⁵⁴³, a progressivement permis de faire émerger une approche européenne insistant sur les garanties devant être apportées lors de l'utilisation des données PNR.

Parmi les divers accords qui ont été conclus à ce sujet, le projet d'accord entre le Canada et l'Union européenne sur le transfert des données personnelles a fait l'objet d'une attention particulière de la part de la doctrine dans la mesure où, outre l'examen de la compatibilité avec le droit de l'Union, l'avis précité de la CJUE se distingue en confrontant l'accord à la Charte des droits fondamentaux pour s'assurer d'un niveau de protection satisfaisant des

⁵⁴¹ Convention de Chicago, Annexe 9, Pratique recommandée 9.23. Lire en ce sens P. BIPLAN, « Les compagnies aériennes entre la nation et la mondialisation », *Hérodote*, 2004, pp. 56-70 ; P. DUPONT, « La souveraineté aérienne et les frontières de la troisième dimension », *Revue défense nationale*, 2023, pp. 157-161.

⁵⁴² Ibidem

⁵⁴³ P. GILLIAUX, « La force obligatoire de la Charte des droits fondamentaux de l'Union européenne, *Revue trimestrielle des droits de l'Homme*, 2022, pp. 69-102.

droits fondamentaux des citoyens européens, notamment du droit au respect à la vie privée et du droit à la protection des données personnelles⁵⁴⁴.

La coopération euro-canadienne a des racines très lointaines. En effet, depuis le 4 avril 1949, le Canada fait partie de l'alliance intergouvernementale pour la sécurité avec les États-Unis et dix pays d'Europe occidentale. Pour mettre fin aux conflits qui ensanglantaient régulièrement l'Europe et qui culminèrent avec la Seconde Guerre mondiale, les responsables politiques européens ont initié un processus d'intégration que nous connaissons aujourd'hui comme l'Union européenne⁵⁴⁵. Le Canada est l'un des plus anciens partenaires des Européens, parmi les pays industrialisés ; un accord entre les deux remontent à 1959⁵⁴⁶. Ce rapprochement semble facilité par une convergence de vue des deux parties sur l'importance accordée au respect des droits fondamentaux dans le cadre de différentes coopérations dans le domaine de la sécurité.

Durant les trente dernières décennies, les mécanismes de dialogue bilatéral se sont traduits par des échanges réguliers entre Européens et Canadiens sur les questions de politique de sécurité, après un déclin constaté à la fin des années 1960, notamment lorsque Pierre Trudeau a réduit de moitié le contingent canadien présent en Europe⁵⁴⁷. Une nouvelle étape de ce dialogue, réalisé dans le cadre de rencontres et de sommets réguliers, a été franchie avec la Déclaration politique et du Plan d'action Canada-EU qui évoquait une « participation accrue du Canada à la nouvelle architecture de sécurité européenne »⁵⁴⁸. Ces dialogues réguliers, qui ont fini par s'institutionnaliser⁵⁴⁹, entre le Canada et l'Union européenne (jadis la Communauté européenne), consacraient une place importante aux questions de sécurité.

Au fil des décennies, cette coopération s'est transformée en un partenariat clé touchant aux divers défis mondiaux. Ces deux parties travaillent également en étroite collaboration dans le cadre du G7 et du G20. Les relations⁵⁵⁰ entre l'Union européenne et le Canada⁵⁵¹ ont pour

⁵⁴⁴ R. TINIERE, « Droits fondamentaux », *Annuaire de droit de l'Union européenne*, 2019, pp. 419-465.

⁵⁴⁵ Union européenne, « Histoire de l'Union européenne 1945-1959 », *Histoire de l'UE*, 2023, en ligne à URL : https://european-union.europa.eu/principles-countries-history/history-eu/1945-59_fr consulté en ligne le 22 février 2022.

⁵⁴⁶ European Union, "EU-Canada relations: Taking forward a vibrant partnership", *EU Factsheet*, 14 June 2021.

⁵⁴⁷ S.ROUSSEL, P. JANURA, « Les relations canado-européennes en matière de sécurité : Nouveau contexte et nouveaux enjeux pour l'UE et le Canada », *Note de recherche*, Centre d'études sur l'intégration et la mondialisation, Université du Québec à Montréal, 2002.

⁵⁴⁸ Ibidem

⁵⁴⁹ Ibid.

⁵⁵⁰ B. THÉRET, "The New EU Social Policies in the Light of the Canadian Experience of Federalism", *Sociétés contemporaines*, 2002, pp. 51-78. Voir également A-S GIJS, C. GIJS, « Des défis structurels aux ambitions nouvelles, le partenariat UE-Afrique du Sud comme archétype des relations UE-pays émergents ? », *Politique européenne*, 2018, pp. 80-119 en ligne à URL : <https://www.cairn.info/revue-politique-europeenne-2018-4-page-80.htm> consulté le 26 octobre 2023.

pilier un accord de partenariat stratégique (APS) et un accord économique et commercial global (AECG). L'APS, entré en vigueur, à titre provisoire, le 1^{er} avril 2017 fixe le cadre d'approfondissement de leur relation politique. Il met à niveau la politique étrangère et la coopération sectorielle à travers 28 thématiques et zones géographiques, allant de la paix et de la sécurité aux droits de l'Homme, au bien-être des citoyens, à la recherche, à l'innovation, à l'éducation, à la lutte contre le changement climatique, à la protection de l'environnement et à la sécurité énergétique.

Cette progression a également été perceptible dans le contenu des accords PNR. Alors que les accords avec les États-Unis prévoient la transmission de 34 rubriques de données PNR, les accords avec le Canada ne visent que 25 catégories. Il s'agit donc d'un champ de données plus limité. Il vise exclusivement des finalités de lutte contre le terrorisme. De plus, les citoyens européens bénéficient d'un droit d'accès et de rectification de leurs données dans les mêmes conditions que les résidents canadiens. Enfin, il est prévu une durée de conservation de celles-ci de trois ans et demi.

L'accord entre l'Australie et l'Union européenne ne prévoit pas beaucoup de différences en termes de droits et d'obligations, même si les finalités de l'accord sont aussi larges que celles prévues dans l'accord avec les États Unis⁵⁵². Il a été reproché à l'avis de la CJUE sur l'accord entre le Canada et l'UE de sacrifier les droits fondamentaux⁵⁵³ sur l'autel des impératifs de prévention des infractions terroristes et des crimes transnationaux⁵⁵⁴. Or, si le juge européen accepte des exceptions vis-à-vis du droit au respect à la vie privée et sur le droit à la protection des données personnelles (section 1), il ne les justifie qu'au nom de la protection de la sécurité publique (section 2).

⁵⁵¹ J. FERGUSSON, « Canada aux marges », *Outre-terre*, 2006, pp. 362-368, en ligne à URL : <https://www.cairn.info/revue-outre-terre2-2016-4-page-362.htm> consulté le 26 octobre 2023.

⁵⁵² P.M. DUPONT, « Les données des dossiers passagers dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 287, Pédone, 2018.

⁵⁵³ L'avis du Contrôleur européen de la protection des données du 1^{er} mai 2008 sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers à des fins répressives, JOUE n° C 110, 1^{er} mai 2008.

⁵⁵⁴ P.M. DUPONT, « Les données des dossiers passagers dans le transport aérien », op. cit.

Section 1 – L’empiètement reconnu sur le droit au respect à la vie privée et sur le droit à la protection des données personnelles

L'évolution des techniques d'information et de communication, bien que bénéfique, peut-être porteuse de menaces sur la protection de la vie privée et des données à caractère personnel⁵⁵⁵ qui font l'objet de dispositions diverses, tant en droit européen qu'en droit national. L'augmentation continue des capacités de conservation, de consultation et d'exploitation de données inquiète. Dans ce contexte, l'Union aspire à veiller au respect permanent du droit fondamental à la protection des données, dans une période où les sociétés mondialisées sont caractérisées par une évolution rapide des technologies de communication et d'information.

La protection des données à caractère personnel et le respect de la vie privée sont des droits fondamentaux européens garantis par l'article 16 du TFUE et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne⁵⁵⁶ qui a été proclamée le 7 décembre 2000 lors du Conseil européen de Nice. Ce texte européen comporte 54 articles qui consacrent les droits fondamentaux des personnes au sein de l'Union européenne. Ces droits sont répartis entre six valeurs individuelles et universelles, constituant le socle de l'identité européenne : dignité, égalité, liberté, solidarité, citoyenneté et justice.

En plus d'enrichir la liste des droits de l'Homme en Europe dans les nouveaux domaines des données à caractère personnel, ce texte européen améliore la protection des droits fondamentaux en étant le premier à intégrer une énumération de tels droits dans un traité⁵⁵⁷. Donnant à la Charte des droits fondamentaux la même valeur juridique que celle des traités, le Traité de Lisbonne a offert à ce texte une force contraignante à l'égard des États membres. Conséquemment, tout citoyen peut se prévaloir de cette Charte en cas de non-respect de ses droits par un pays européen.

Le Parlement européen a constamment souligné l'importance de trouver un équilibre entre le renforcement des mesures de sécurité et la protection des droits fondamentaux, en particulier

⁵⁵⁵ C. GUERRIER, « Les aspects techniques de la régulation des données personnelles : la question du numéro IP », *LEGICOM*, 2009, pp. 127-141. Voir aussi N. TILLI, La protection des données à caractère personnel, *Documentaliste-Sciences de l'information*, 2013, pp. 62-69 ; D. BATORSKI, Z. SMOREDA, « La diffusion des technologies d'information et de communication, Une enquête longitudinale en Pologne », *Réseaux*, 2007, pp. 193-221 ; N. MALLET-POUJOL, « Protection des données personnelles et droit à l'information », *LEGICOM*, 2017, pp. 49-59.

⁵⁵⁶ Charte des droits fondamentaux de l'Union européenne, 2000.

⁵⁵⁷ P. GAÏA, « La Charte des droits fondamentaux de l'Union européenne », *Revue française de droit constitutionnel*, 2004, pp. 227-246, en ligne à URL : <https://www.cairn.info/revue-francaise-de-droit-constitutionnel-2004-2-page-227.htm?ref=doi> consulté le 31 octobre 2023.

en ce qui concerne la protection des données personnelles⁵⁵⁸. En 2018, de nouvelles règles européennes ont été adoptées en la matière⁵⁵⁹. Par ailleurs, des dispositions spécifiques relatives à la protection des données ont également été intégrées à des actes législatifs sectoriels telle la directive PNR. En outre, des recherches préparées pour les parlementaires européens indiquent que le droit européen relatif à la régulation des flux de données contribue « à hauteur de 51,6 milliards d’euros par an au PIB de l’Union européenne »⁵⁶⁰.

Contesté devant la CJUE (sous-section 1), l’accord PNR conclu entre l’Union européenne et le Canada fait l’objet d’un avis dans lequel les juges de Luxembourg ont admis une entorse aux droits fondamentaux des passagers. Il semblerait donc qu’il s’agisse avant tout d’une question d’équilibre. Ailleurs dans le monde, notamment dans les pays de la Ligue arabe, la conclusion d’accords PNR avec d’autres pays est encore absente, bien que parfois évoquée (sous-section 2).

Sous-section 1 – Un accord PNR euro-canadien objet de contestation

Les institutions européennes, en exprimant leur réticence face à l’accord PNR euro-canadien, ont simultanément reconnu l’ingérence significative que cet accord représente pour les droits fondamentaux des citoyens.

§ 1 – Une réticence des institutions européennes vis-à-vis de l’accord PNR euro-canadien

À l’image de l’accord PNR entre l’Union européenne et les États-Unis, l’accord avec le Canada s’est accompagné de tâtonnements juridiques. Un premier accord à durée limitée avait été conclu en 2005. À son terme, en septembre 2009⁵⁶¹, la Commission européenne a entamé

⁵⁵⁸ Communication de la Commission du 24 juin 2020 intitulée «La protection des données: un pilier de l’autonomisation des citoyens et de l’approche de l’Union à l’égard de la transition numérique, deux années d’application du règlement général sur la protection des données» (SWD(2020)0115).

⁵⁵⁹ Le règlement général sur la protection des données, officiellement 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, est un règlement de l’Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Lire en sens A. DIEHL, « Le GDPR, cette nouvelle loi qui va tout changer », *Abondance, lettre Recherche et Référencement*, avril et mai 2017, en ligne à URL : <http://recherche-referencement.abondance.com/2017/04/le-gdpr-cette-nouvelle-loi-qui-va-tout.html> consulté le 31 octobre 2023 ; G. ZIGNANI, « Protection des données : le législateur appelé à intervenir rapidement », *La Gazette des communes*, 15 mars 2017.

⁵⁶⁰ U. BUX, M. MACIEJEWSKI, « La protection des données à caractère personnel », *Fiches thématiques sur l’Union européenne*, Parlement européen, juin 2022, en ligne à URL : <https://www.europarl.europa.eu/factsheets/fr/sheet/157/la-protection-des-donnees-a-caractere-personnel> consulté en ligne le 20 février 2022.

⁵⁶¹ Conseil de l’Union européenne, déc. n° 2006/230/CE, 18 juillet 2005, relative à la conclusion de l’accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données IPV/DP : JOUE n° L 82, 21 mars 2006, p. 14.

de nouvelles négociations dès la fin de l'année 2010⁵⁶² débouchant sur un second accord paraphé en mai 2013 et signé par le Conseil des ministres de l'UE et le Canada le 25 juin 2014⁵⁶³. Toutefois, ce nouvel accord n'a pas fait l'unanimité⁵⁶⁴. Le Contrôleur européen de la protection des données a ainsi énoncé des réserves quant à ce projet, notamment concernant, d'une part, « la nécessité et la proportionnalité des systèmes PNR et des transferts massifs de données PNR aux pays tiers » et, d'autre part, la protection des données sensibles, le choix de la base juridique et le droit des passagers aériens⁵⁶⁵.

Cette inquiétude s'est concrètement exprimée lorsque le Parlement européen a saisi la Cour de justice pour avis⁵⁶⁶, conformément à l'article 218 § 11 TFUE, après avoir été saisi pour approbation⁵⁶⁷. Le rapporteur parlementaire justifia ce recours en ces termes : « Nous voulons une certitude juridique pour les citoyens de l'UE et les transporteurs aériens, non seulement vis-à-vis de l'accord PNR avec le Canada mais également comme référence pour les futurs accords avec d'autres pays, qui demandent la collecte massive de données personnelles de citoyens européens »⁵⁶⁸.

En effet, les futurs accords étaient fortement susceptibles d'inclure des pays dont la culture juridique, notamment en termes de respect des droits fondamentaux, allait différer de la culture juridique inspirant l'Union européenne. Le rapporteur européen a souligné que des pays comme la Russie, le Mexique et la Corée, qui ont des règles de protection des données moins strictes, pourraient également chercher à négocier leurs propres accords sur les données de passagers. Elle a donc jugé qu'il était impératif que tout accord, qu'il soit actuel ou futur, soit en conformité avec les traités de l'Union européenne et les droits fondamentaux, et ne serve pas à affaiblir les normes européennes en matière de protection des données⁵⁶⁹.

De plus, l'accord PNR entre l'UE et les États-Unis, élaboré dans un contexte temporel différent, offre un cadre distinct qui mérite d'être examiné en parallèle avec celui de l'UE et du Canada. Tout d'abord l'accord entre américains et européens a été nécessaire afin que les

⁵⁶² Résolution du Parlement européen du 5 mai 2010 sur le lancement des négociations sur les accords relatifs aux données des passagers aériens (PNR) avec les États-Unis, l'Australie et le Canada, 5 mai 2010, Bruxelles.

⁵⁶³ Parlement européen, « Actualité, Accord UE-Canada sur les données des passagers aériens : saisine de la Cour de la justice européenne », 25 novembre 2014.

⁵⁶⁴ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁵⁶⁵ Avis du Contrôleur européen de la protection des données sur les propositions de décisions du Conseil relatives à la conclusion et à la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, C 51/12, 22 février 2014.

⁵⁶⁶ CJUE, Avis 1/15 de la Cour (grand chambre), 26 juillet 2017, pt.1.

⁵⁶⁷ TFUE, article 218 § 11. Lire en ce sens.

⁵⁶⁸ Parlement européen, « Accord UE-Canada sur les données des passagers aériens : saisine de la Cour de la justice européenne », *Actualité*, 25 novembre 2014.

⁵⁶⁹ *Ibidem*

compagnies aériennes européennes ne soient pas placées en porte-à-faux devant la législation américaine votée après les attentats du 11 septembre 2001. Comme l'accord euro-américain⁵⁷⁰, l'accord entre le Canada et l'Union européenne est passé par plusieurs phases et a été souvent critiqué par les institutions européennes en raison du peu de garanties qu'il offrait en termes de protection des droits fondamentaux, en particulier de la vie privée et des données personnelles⁵⁷¹.

L'accord PNR euro-américain a été conclu dans le cadre du troisième pilier qui regroupe les domaines de police et de justice. Le ministère de l'Intérieur américain a obtenu le droit de transférer les données PNR à d'autres autorités gouvernementales. Or, ce même ministère a accès, dans des circonstances exceptionnelles, aux données sensibles, c'est-à-dire celles pouvant révéler l'origine raciale ou ethnique, les convictions religieuses, les opinions politiques ou les données de santé des passagers. Par ailleurs, les finalités du système ainsi mis en place sont très larges et évolutives. Enfin, les données sont conservées sept ans, puis huit ans supplémentaires en cas de besoin, soit un total possible de quinze années, sans que des garanties s'agissant de leur destruction soit apportées au-delà de ce délai⁵⁷².

À titre de comparaison, l'accord PNR entre l'UE et l'Australie a suscité des réactions plus positives, offrant un point de contraste intéressant avec les retours mitigés concernant l'accord entre l'UE et le Canada. Un document de la Commission européenne, en date du 10 juillet 2014⁵⁷³, a permis d'évaluer la mise en œuvre de l'accord conclu entre l'Union européenne et l'Australie. Ce rapport de la Commission était destiné au Parlement européen et au Conseil et portait sur le traitement ainsi que le transfert de données des dossiers passagers par les transporteurs aériens au service australien des douanes et de la protection des frontières⁵⁷⁴.

Ce document constata que l'Australie appliquait pleinement l'accord, dans les conditions prévues. Il releva notamment que les autorités australiennes remplissaient leurs obligations en ce qui concerne les garanties en matière de protection des données prévues par l'accord et

⁵⁷⁰ Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure, 2012.

⁵⁷¹ S. PEYROU, « Accord PNR UE-Canada : validation par la CJUE du système PNR, des modalités à revoir ! (réflexions sur l'avis 1/15 de la CJUE, 26 juillet 2017) », *GDR-ELSJ*, 28 juillet 2017, en ligne à URL : <https://www.gdr-elsj.eu/2017/07/28/informations-generales/accord-pnr-ue-canada-validation-cjue-systeme-pnr-modalites-a-revoir-reflexions-lavis-115-de-cjue-26-juillet-2017/>, consulté le 31 octobre 2023.

⁵⁷² S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.

⁵⁷³ Document de la Commission COM (2014) 458 final du 10 juillet 2014, Rapport de la Commission au Parlement européen et au Conseil sur l'examen conjoint de la mise en œuvre de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières.

⁵⁷⁴ Ibidem.

traitaient les données des dossiers passagers selon les conditions énoncées⁵⁷⁵. Par ailleurs, il a été constaté que l'Australie ne traitait aucune donnée sensible contenue dans les données des passagers aériens qu'elle obtenait, conformément à l'accord. Par ailleurs, il a été indiqué que l'Australie cherchait encore activement à perfectionner l'identification et la suppression automatisée des données dites sensibles.

L'Australie a été reconnue pour son application exemplaire de la méthode « push », avec une mention spéciale de l'Union européenne pour avoir étendu cette méthode à l'ensemble des compagnies aériennes, même celles non couvertes par l'accord⁵⁷⁶. De plus, l'Australie est considérée comme un leader dans le développement et la promotion de la structure de message standard PNRGOV au niveau mondial. Son engagement actif avec les compagnies aériennes ainsi qu'avec des organisations internationales telles que l'Organisation mondiale des douanes (OMD), l'Organisation de l'aviation civile internationale (OACI) et l'Association du transport aérien international (IATA) vise à normaliser la transmission des données PNR à l'échelle mondiale⁵⁷⁷.

Par ailleurs, l'accord PNR signé entre Européens et Canadiens a été interprété dans un contexte différent de celui de l'accord conclu avec les Américains étant donné qu'entretemps, le Traité de Lisbonne est entré en vigueur. Ce dernier a introduit l'article 16 du TFUE qui prévoit que « Toute personne a droit à la protection des données à caractère personnel la concernant »⁵⁷⁸. Dès lors, « les questions relatives à la base juridique sont ainsi posées en des termes différents de ceux de l'arrêt de 2006 »⁵⁷⁹, rappelle Vincent Correia⁵⁸⁰.

L'inépuisable débat entre liberté et sécurité, exacerbé par les attentats terroristes qui ont eu lieu au cours de la dernière décennie et la multiplication des législations des États européens pour y faire face, a inspiré les conclusions de l'avocat général vis-à-vis de la demande d'avis formulé par le Parlement européen à la CJUE à propos de l'accord PNR signé entre l'Union européenne et le Canada⁵⁸¹. Celles-ci, tout en condamnant en l'état la conclusion de l'accord PNR, ont laissé la porte ouverte à une acceptation de celui sous certaines conditions. Dans son argumentation détaillée, l'avocat général s'est appuyé sur la jurisprudence de la Cour de justice en matière de protection des droits fondamentaux, notamment les arrêts Digital Rights

⁵⁷⁵ Ibid.

⁵⁷⁶ Ibid.

⁵⁷⁷ Ibid.

⁵⁷⁸ Traité sur le fonctionnement de l'Union européenne, 26 octobre 2012.

⁵⁷⁹ CJCE, 30 mai 2006, Parlement c/ Conseil.

⁵⁸⁰ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁵⁸¹ Conclusion de l'avocat général Mengozzi présentées le 8 septembre 2016, ECLI :EU :C :2016 :656.

Ireland⁵⁸² (C-293/12 & C-594/12, 8 avril 2014) et Schrems⁵⁸³ (C-362/14, 6 octobre 2015), qui ont permis au juge européen d'affirmer haut et fort le droit au respect de la vie privée et le droit à la protection des données personnelles qui figurent respectivement aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Pour l'avocat général, le système du PNR peut être jugé pertinent à la condition que soient écartées les dispositions qui contreviennent à la Charte⁵⁸⁴.

L'avocat général souligna, tout d'abord, que « la nature des données PNR faisant l'objet de l'accord envisagé ne permet pas de tirer des conclusions précises sur le contenu essentiel de la vie privée des personnes concernées » (§ 186 de l'avis), et a estimé que l'antagonisme vis-à-vis des droits fondamentaux contenue dans l'accord ne portait pas atteinte au contenu même du droit fondamental, au respect de la vie privée (article 7 de la Charte) ou à la protection des données personnelles (article 8) et, par conséquent, ne violait pas l'article 52 § 1 de la Charte.

Ce constat se lit à l'aune de la jurisprudence Digital Rights Ireland dans laquelle la CJUE avait invalidé la directive 2006/24/CE relative à la rétention des données de communication électroniques dès lors que la quantité et la qualité des données, dont les métadonnées de communication, recueillies et traitées, donnaient lieu à une « cartographie aussi fidèle qu'exhaustive (...) des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée », pour reprendre les mots de l'avocat général Cruz Villalón dans ses conclusions. Or, dans l'avis sur le PNR euro-canadien, l'avocat général a été forcé de constater que « l'ingérence que comporte l'accord envisagé est moins vaste que celle prévue par la directive 2006/24 tout en étant également moins intrusive dans la vie quotidienne de chaque personne » (§ 240). C'est ce constat qui a ouvert la possibilité de l'existence d'un système PNR, si toutefois l'accord satisfait les exigences de protection des droits fondamentaux qui découlent de la Charte et rappelées dans l'arrêt Digital Rights Ireland⁵⁸⁵.

Cela étant, l'avocat général s'est montré circonspect sur l'aspect « indifférencié et généralisé » que comporte l'accord PNR conclu entre l'Union européenne et le Canada. C'est pourquoi il s'est livré à une analyse minutieuse du système PNR en relevant que,

⁵⁸² Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a., CJUE, Affaires jointes C-293/12 et C-594/12, 8 avril 2014.

⁵⁸³ CJUE, Maximilian Schrems c/ Data Protection Commissioner, affaire C-362/14, 6 octobre 2015.

⁵⁸⁴ S. PEYROU, « Accord PNR UE-Canada : validation par la CJUE du système PNR, des modalités à revoir ! », *GDR-ELSJ*, 28 juillet 2017, en ligne à URL : <http://www.gdr-elsj.eu/2017/07/28/informations-generales/accord-pnr-ue-canada-validation-cjue-systeme-pnr-modalites-a-revoir-reflexions-lavis-115-de-cjue-26-juillet-2017/> consulté le 21 août 2023.

⁵⁸⁵ CJUE, Digital Rights Ireland, 8 avril 2014.

« contrairement aux personnes dont les données faisaient l'objet du traitement prévu par la directive 2006/24, toutes celles relevant de l'accord envisagé empruntent volontairement un moyen de transport international à destination ou en provenance d'un pays tiers, moyen de transport qui est lui-même, de manière récurrente malheureusement, vecteur ou victime d'actes de terrorisme ou de criminalité transnationale grave, ce qui nécessite l'adoption de mesures assurant un niveau de sécurité élevé de l'ensemble des passagers » (§ 242). Cet avis a été l'occasion pour l'avocat général d'imaginer un système comprenant des mécanismes plus restrictifs mais il n'a pu s'empêcher de constater qu'« aucune autre mesure qui, tout en limitant le nombre de personnes dont les données PNR sont traitées automatiquement par l'autorité canadienne compétente, serait susceptible d'atteindre avec une efficacité comparable le but de sécurité publique poursuivi par les parties contractantes n'a été portée à la connaissance de la Cour dans le cadre de la présente procédure » (§ 244). Par conséquent, il a pu conclure que « tout bien pesé, il me semble donc que, de manière générale, le champ d'application personnel de l'accord envisagé ne saurait être circonscrit davantage, sans que cela porte préjudice à l'objet même des régimes PNR » (§ 245)⁵⁸⁶.

L'intitulé du communiqué de presse⁵⁸⁷ de la Cour de justice retranscrit clairement l'idée général de l'avis : « Selon l'avocat général Mengozzi, l'accord (...) ne peut pas être conclu sous sa forme actuelle ». La tournure de cette déclaration indique que si la pertinence du système PNR n'est pas remise en question, l'accord entre Européens et Canadiens est tout de même caractérisé par des manquements s'agissant du respect des droits fondamentaux, ce qui oblige les parties à une renégociation de l'accord afin de le rendre conforme au cadre juridique européen, à la Charte plus précisément. L'avocat général a construit sa réflexion en deux temps.

Dans un premier temps, l'avocat général a reconnu que l'accord était compatible avec la Charte des droits fondamentaux de l'UE⁵⁸⁸, y compris le droit au respect de la vie privée et familiale ainsi que le droit à la protection des données personnelles, sous réserve du respect de certaines conditions⁵⁸⁹.

⁵⁸⁶ CJUE, Communiqué de presse n° 89/16, Conclusions de l'avocat général dans la demande d'avis 1/15, Luxembourg, le 8 septembre 2016.

⁵⁸⁷ Ibidem

⁵⁸⁸ Ibid.

⁵⁸⁹ J.-P. FOEGLE, « Protection des données personnelles : un droit fondamental menacé », *Plein droit*, 2016, pp. 41-48, en ligne à URL : <https://www.cairn.info/revue-plein-droit-2016-3-page-41.htm> consulté le 31 octobre 2023. Sur cette jurisprudence européenne relative aux données personnelles et les droits fondamentaux, voir J-P FOEGLE, « Chronique du droit "Post-Snowden" : la CJUE et la CEDH sonnent le glas de la surveillance de masse », *La Revue des droits de l'Homme*, Actualités Droits-Libertés, 30 mars 2016, en ligne à URL : <https://journals.openedition.org/revdh/2074> consulté le 13 juillet 2016.

Premièrement, les catégories de données PNR des passagers aériens doivent être définies de manière claire et précise, avec l'exclusion explicite des données sensibles du champ d'application de l'accord. Cependant, l'avocat général a observé que certaines catégories énoncées dans l'accord étaient formulées de manière trop large, voire excessivement vague. C'est le cas notamment de la rubrique 7 relative à « toutes les coordonnées disponibles » et de la rubrique 17 relative aux « remarques générales » que sont susceptibles de contenir des données sensibles, comme la préférence pour les repas à bord de l'avion qui peuvent révéler les convictions religieuses du passager aérien. Pour cette raison, l'avocat général souhaite que ces données sensibles soient exclues du champ d'application de l'accord. Il observa également, de manière pragmatique, qu'un membre d'un réseau terroriste éviterait probablement de divulguer des informations compromettantes de cette manière, ce qui entraînerait que seules des personnes innocentes, utilisant ces services sans méfiance et pouvant être injustement soupçonnées en raison de leur appartenance religieuse, seraient finalement visées⁵⁹⁰.

Deuxièmement, l'avocat général a préconisé une liste exhaustive des infractions correspondant aux formes graves de criminalité transnationale dans l'accord, afin de délimiter clairement ses objectifs. Troisièmement, il a estimé nécessaire que l'accord identifie de manière précise l'autorité responsable du traitement des données PNR, afin de garantir leur protection et leur sécurité. Il a suggéré que l'expression « autorité canadienne compétente » soit préférée à des termes plus vagues pour désigner ces entités.

Quatrièmement, il a été jugé que le nombre de personnes ciblées devrait être largement limité de manière non discriminatoire, de sorte qu'il ne concerne que celles pour lesquelles existe un soupçon raisonnable de participation à des actes terroristes ou à des crimes transnationaux graves. Cette condition vise à aborder le problème des faux positifs, qui sont inévitablement générés par les algorithmes utilisés dans le mécanisme proactif de détection des passagers suspects. Cependant, il est reconnu que ces erreurs ne sont pas faciles à éviter⁵⁹¹.

Cinquièmement, l'avocat général a estimé que l'accord doit spécifier que « seuls les fonctionnaires de l'autorité canadienne compétente sont habilités à accéder aux données PNR et prévoit des critères objectifs permettant d'en préciser le nombre ». Cette condition

⁵⁹⁰ S. PEYROU, « Accord PNR UE-Canada : validation par la CJUE du système PNR, des modalités à revoir ! », *GDR-ELSJ*, 28 juillet 2017, en ligne à URL : <http://www.gdr-elsj.eu/2017/07/28/informations-generales/accord-pnr-ue-canada-validation-cjue-systeme-pnr-modalites-a-revoir-reflexions-lavis-115-de-cjue-26-juillet-2017/> consulté le 21 août 2023

⁵⁹¹ La pratique du profilage a fait l'objet de nombreux commentaires, notamment depuis que le RGPD s'attache à réglementer cette pratique. Voir en ce sens. E. GUISSART, J-F. HENROTTE, « Profilage : la segmentation jusque dans le régime du RGPD », *PIN CODE*, 2020, pp. 10-18.

complète la précédente et vise à clarifier le nombre ainsi que la qualité des autorités qui ont accès aux données personnelles des passagers aériens.

Sixièmement, l'accord doit clairement spécifier les raisons objectives justifiant la nécessité de conserver toutes les données PNR des passagers pour une période maximale de cinq ans⁵⁹². Il est essentiel que, si ces données doivent être conservées pendant toute cette durée, celles permettant d'identifier directement un passager soient anonymisées par masquage. Cette durée de conservation est jugée nécessaire pour atteindre les objectifs visés, comme l'a souligné l'arrêt Digital Rights Ireland.

Septièmement, l'avocat général jugea essentiel de mettre en place une autorité indépendante ou une juridiction canadienne pour vérifier, au préalable et au cas par cas, si l'autorité canadienne compétente peut partager les données PNR avec d'autres autorités publiques, qu'elles soient canadiennes ou étrangères. Si ces données concernent un citoyen de l'Union européenne, il est également nécessaire d'en informer à l'avance les autorités compétentes de l'État membre concerné et/ou la Commission européenne.

Huitièmement, l'accord doit inclure une règle claire et précise garantissant qu'une autorité indépendante ait systématiquement la possibilité de vérifier que les droits à la vie privée et à la protection des données personnelles des passagers dont les données PNR sont traitées sont respectés.

Ensuite, en neuvième point, l'avocat général a exigé que l'accord indique explicitement que les demandes d'accès, de rectification ou d'annotation soumises par des passagers situés hors du territoire canadien doivent pouvoir être adressées à une autorité publique indépendante.

Dans un second temps, l'avocat général a constaté que certaines dispositions de l'accord sont manifestement contraires à la Charte des droits fondamentaux de l'Union européenne et susceptibles de créer des obstacles lors de la renégociation de l'accord. En effet, ces dispositions ont été critiquées pour plusieurs raisons. Tout d'abord, elles permettent d'étendre les possibilités de traitement des données PNR au-delà de ce qui est strictement nécessaire, en s'éloignant de l'objectif principal de sécurité publique fixé par l'accord, à savoir la prévention et la détection des actes terroristes et des formes graves de criminalité transnationale.

⁵⁹² Conclusions de l'Avocat général M. Paolo Mengozzi, présentées le 8 septembre 2016, Avis 1/15 (demande d'avis présentée par le Parlement européen), concernant le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers [Passenger Name Record (PNR)], compatibilité avec l'article 16 TFUE et les articles 7, 8 et 52(1) de la Charte des droits fondamentaux de l'Union européenne.

De plus, elles autorisent le Canada à traiter, utiliser et conserver des données PNR contenant des informations sensibles. Par ailleurs, elles permettent au Canada de divulguer toute information sans exiger de lien direct avec l'objectif de sécurité publique poursuivi par l'accord. En outre, ces dispositions permettent au Canada d'utiliser ces données sur une période maximale de cinq ans pour toute action, vérification, enquête ou procédure judiciaire, toujours sans exiger un lien direct avec l'objectif de sécurité publique défini par l'accord.

Enfin, elles acceptent que le transfert de données PNR à une autorité publique étrangère puisse se faire sans que l'autorité canadienne compétente, sous la supervision d'une autorité indépendante, ait préalablement vérifié que l'autorité étrangère ne pourrait pas transmettre les données à une autre entité étrangère⁵⁹³.

Les reproches formulés par l'avocat général Mengozzi, sur l'accord relatif au transfert des données des dossiers passagers entre l'Union européenne et le Canada, se sont fondés sur « des enseignements issus des arrêts Digital Rights Ireland et Schrems », tel que le rappelle le communiqué de presse⁵⁹⁴. Ses conclusions l'ont amené à espérer un contrôle plus strict de l'accord vis-à-vis du droit au respect de la vie privée et familiale et du droit à la protection des données à caractère personnel.

L'avocat général souligne que, dans un monde où les technologies modernes permettent aux autorités publiques de mettre en place des méthodes très sophistiquées de surveillance et d'analyse des données personnelles, sous couvert de lutte contre le terrorisme et la criminalité transnationale, la protection des droits fondamentaux devient d'autant plus essentielle. Cette menace potentielle sur les libertés individuelles exige que le juge européen veille à ce que tout accord international dans ce domaine assure un équilibre approprié entre la nécessité de garantir la sécurité publique et celle de préserver un niveau élevé de protection de la vie privée et des données personnelles de chaque individu⁵⁹⁵.

§ 2 – Une reconnaissance de l'ingérence dans les droits fondamentaux des passagers aériens

En 2017, la CJUE a conclu que si le transfert, la conservation et l'utilisation systématiques des données de dossiers passagers que prévoit l'accord PNR sont pour l'essentiel admissibles, plusieurs dispositions du projet ne sont pas conformes aux exigences découlant des droits

⁵⁹³ Ibidem.

⁵⁹⁴ CJUE, Communiqué de presse n° 89/16, Conclusions de l'avocat général dans la demande d'avis 1/15, Luxembourg, le 8 septembre 2016. Voir aussi : J. DUTHEIL DE LA ROCHERE, « Droit au juge, accès à la justice européenne », *Pouvoirs*, 2001, pp. 123-141. Pour une étude plus développée sur cette question, voir P. VAN DIJK, « Access to Court », in R.S.J. Macdonald et al. (ed.), *The European System of Protection of Human Rights*, Kluwer, 1993, pp. 345-373.

⁵⁹⁵ Ibidem

fondamentaux de l'Union européenne⁵⁹⁶. Les juges de Luxembourg ont donc considéré que « l'accord PNR ne peut pas être conclu sous sa forme actuelle en raison de l'incompatibilité de plusieurs de ses dispositions avec les droits fondamentaux reconnus par l'Union »⁵⁹⁷.

Pour la Cour européenne, si les ingérences dans les droits fondamentaux des passagers aériens européens sont justifiées car elles visent à garantir la sécurité publique en luttant contre les actes terroristes et les crimes transnationaux, « plusieurs dispositions de l'accord ne sont pas limitées au strict nécessaire et ne prévoient pas des règles claires et précises ». En particulier, le transfert des données dites « sensibles », c'est à dire les données révélant « l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale » ou concernant « l'état de santé ou la vie sexuelle d'une personne », dont le transfert vers le Canada devrait être justifié par d'autres motifs que ceux visant la protection de la sécurité publique, est incompatible avec les droits fondamentaux du fait d'un risque de traitement contraire au principe de non-discrimination⁵⁹⁸.

D'autre part, si le traitement des données des dossiers passagers présents au Canada ou en partance du pays « ne dépasse pas les limites du strict nécessaire du fait de la conservation ou de l'utilisation systématique » de ces données, la Cour a estimé que leur utilisation, pendant le séjour au Canada, « doit se fonder sur des circonstances nouvelles justifiant cette utilisation » afin de « protéger les données contre les risques d'abus ». Les juges européens ont ici rappelé que si le traitement des données des dossiers passagers dicté par un objectif de sécurité publique contre les menaces terroristes doit faciliter et accélérer les contrôles de sécurité notamment aux frontières, il ne doit pas pour autant sacrifier les droits fondamentaux des passagers aériens.

L'originalité de cet accord est qu'il fut le premier à être analysé par la Cour au regard des nouveaux textes européens⁵⁹⁹. En effet, pour l'avocat général Mengozzi, c'est « la première fois que la Cour [doit] se prononcer sur la compatibilité d'un projet d'accord international avec les droits fondamentaux consacrés par la Charte des droits fondamentaux de l'Union européenne »⁶⁰⁰. Cette charte a été au cœur de la réflexion des juges européens dans les

⁵⁹⁶ CJUE, 26 juillet 2017, avis 1/15.

⁵⁹⁷ CJUE, Communiqué de presse n° 89/16, Conclusions de l'avocat général dans la demande d'avis 1/15, Luxembourg, le 8 septembre 2016.

⁵⁹⁸ E. MUIR, « L'action juridique de l'union européenne dans la lutte contre les discriminations », *Migrations société*, 2010, pp. 87-104 ; M-T. LANQUETIN, « Le droit de la non-discrimination en Europe », *Travail et genre dans le monde*, 2013, pp. 52-61.

⁵⁹⁹ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁶⁰⁰ Ibidem

jurisprudences Digital Rights Ireland⁶⁰¹, Schrems⁶⁰² et Tele2 Sverige⁶⁰³ ; la première ayant abouti à l'annulation de la directive n° 2006/24/CE. L'avis sur l'accord euro-canadien a donc été une occasion pour la Cour de réaffirmer le caractère fondamental du droit à la protection des données personnelles.

Ce faisant, la Cour a répondu au doute qu'avait émis le Parlement européen quant à la compatibilité de l'accord PNR Canada-EU avec l'article 16 TFUE ainsi que les articles 7, 8 et 52 de la Charte des droits fondamentaux⁶⁰⁴. De cet avis, il ressort que l'article 16 TFUE « constitue bien une base juridique appropriée pour conclure des accords portant sur le transfert et le traitement des données des dossiers passagers, il n'est pas mobilisé par les juges de Kirchberg au titre de la protection des droits fondamentaux »⁶⁰⁵. En fait, c'est le jeu combiné des articles de la Charte des droits fondamentaux qui permet de garantir la protection du droit au respect de la vie privée et familiale et du droit à la protection des données à caractère personnel, tout en prévoyant des limites lorsqu'elles remplissent les conditions posées par l'article 52 de ce même texte. Ainsi, la Cour a été conduite à considérer implicitement que l'article 8 de la Charte « fait office de *lex specialis* au regard de l'article 16 TFUE »⁶⁰⁶.

Par ailleurs, la Cour a fait référence aux articles 7 et 8 de la Charte en considérant que « les données PNR comportant, ainsi, des informations sur des personnes physiques identifiées, à savoir les passagers aériens empruntant des vols entre l'Union et le Canada, les différents traitements dont, selon l'accord envisagé, celles-ci peuvent faire l'objet, à savoir leur transfert depuis l'Union vers le Canada, l'accès à celles-ci en vue de leur utilisation ou encore leur conservation, affectent le droit fondamental au respect de la vie privée, garanti à l'article 7 de la Charte. En effet, ce droit se rapporte à toute information concernant une personne physique identifiée ou identifiable »⁶⁰⁷ ; avant de considérer, au point 123 de l'avis, que « les traitements des données PNR visés par l'accord envisagé relèvent également de l'article 8 de la Charte en raison du fait qu'ils constituent des traitements des données à caractère personnel au sens de cet article et doivent, par suite, nécessairement satisfaire aux exigences de

⁶⁰¹ Digital Rights Ireland Ltd c/ Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a., CJUE, Affaires jointes C-293/12 et C-594/12, 8 avril 2014.

⁶⁰² Maximilian Schrems c/ Data Protection Commissioner, CJUE, affaire C-362/14, 6 octobre 2015

⁶⁰³ Tele2 Sverige AB c/ Post- och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson e.a., CJUE, Affaires jointes C-203/15 et C-698/15, 21 décembre 2016.

⁶⁰⁴ V. CORREIA, op. cit.

⁶⁰⁵ Ibidem

⁶⁰⁶ Ibid.

⁶⁰⁷ CJUE, 26 juillet 2017, avis 1/15, point 122.

protection des données prévues audit article »⁶⁰⁸. Les juges européens ont ainsi utilisé, de manière concomitante, les articles 7 et 8 de la Charte pour reconnaître les atteintes aux droits fondamentaux en matière de protection des données à caractère personnel, conformément à la jurisprudence antérieure dans ce domaine qui invoque de façon systématique les deux droits conjointement. En effet, la jurisprudence de la Cour a admis cela dans le passé, considérant qu'« il découle de ces dispositions, lues conjointement, que, en principe, est susceptible de constituer une atteinte auxdits droits tout traitement des données à caractère personnel par un tiers »⁶⁰⁹. La mobilisation de ces éléments conjointement confirme la volonté de la Cour d'élargir le périmètre d'application de la protection des données à caractère personnel⁶¹⁰.

Pour établir la réalité des risques d'empiètement sur le droit à la vie privée, la Cour a procédé à une lecture systématique et globale des données des passagers aériens ainsi que de l'utilisation de celles-ci par les autorités canadiennes. Elle a insisté sur les conséquences pratiques de la collecte⁶¹¹ et de l'utilisation des données PNR par les autorités canadiennes selon une approche *in globo* à la place d'une approche atomistique des données, qui est considérée comme étant plus rigoureuse sur le terrain du droit⁶¹². En effet, l'approche atomistique ne permet pas de saisir les risques liés à l'utilisation et au traitement des données PNR, car ces dernières, « prises isolément, ne paraissent pas pouvoir révéler des informations importantes sur la vie privée des personnes concernées »⁶¹³. Toutefois, lorsqu'elles sont « prises ensemble »⁶¹⁴, elles peuvent « révéler un itinéraire de voyage complet, des habitudes de voyage, des relations existantes entre deux ou plusieurs personnes ainsi que des informations sur la situation financière des passagers aériens, leurs habitudes alimentaires ou leur état de santé, et pourraient même fournir des informations sensibles sur ces passagers »⁶¹⁵.

Cette démarche de la Cour reprend le raisonnement suivi dans la jurisprudence Digital Rights Ireland et Tele2 Sverige à propos de la conservation des données des abonnés et utilisateurs

⁶⁰⁸ Ibidem, point 123.

⁶⁰⁹ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁶¹⁰ Ibidem

⁶¹¹ Sur la collecte des données à caractère personnel, voir les travaux d'Emmanuel Derieux, notamment E. DERIEUX, « Vie privée et données personnelles – Droit à la protection et "droit à l'oubli" face à la liberté d'expression », *Les nouveaux cahiers du Conseil constitutionnel*, 2015, pp. 21-31, en ligne à URL : <https://www.cairn.info/revue-les-nouveaux-cahiers-du-conseil-constitutionnel-2015-3-page-21.htm> consulté le 31 octobre 2023.

⁶¹² V. CORREIA, op. cit.

⁶¹³ CJUE, 26 juillet 2017, avis 1/15, Point 128.

⁶¹⁴ Ibidem

⁶¹⁵ Ibid.

des moyens de communication mobile et électronique⁶¹⁶. Dans l'avis, la Cour souligna la possibilité de regrouper les données PNR avec d'autres catégories de données, sur la durée de conservation des données ou bien sur l'analyse systématique par des moyens automatisés⁶¹⁷. Partant de ce constat, et sans développer longuement son argumentation, la Cour a considéré que le transfert des données PNR vers le Canada constituait une ingérence dans les droits fondamentaux des citoyens européens⁶¹⁸. Cette décision lui a permis de se distinguer de son arrêt Parlement contre Conseil de 2006⁶¹⁹ qui ne pouvait mettre en avant la fundamentalité des droits que la Charte permet aujourd'hui.

Sous-section 2 – L'absence de développement d'accords PNR avec les pays de la Ligue arabe

L'absence de développement d'accords PNR avec les pays de la Ligue arabe, en particulier ceux du Golfe qui abritent certaines des plus grandes compagnies aériennes mondiales⁶²⁰, constitue un enjeu non-négligeable dans cette thèse. Un potentiel accord entre l'Union européenne et les pays de la Ligue arabe, qui se déclarent également engagés dans la lutte contre le terrorisme, soulève des interrogations⁶²¹. Ces accords posent la question de l'équilibre entre sécurité et protection des données dans un contexte international élargi. À ce jour, aucun accord PNR n'a encore été établi entre les pays de la Ligue arabe et l'Union européenne.

§ 1 – La Ligue arabe, une organisation intergouvernementale régionale faiblement protectrice des droits fondamentaux

Le 22 mars 1945, six États arabes (l'Arabie Saoudite, l'Égypte, l'Irak, la Jordanie (connue, à l'époque, sous le nom de Transjordanie), le Liban et la Syrie) ont adopté le Pacte de la Ligue des États arabes fondant l'une des plus anciennes organisations internationales au fonctionnement intergouvernemental agissant à travers plusieurs organes : le Conseil de la

⁶¹⁶ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁶¹⁷ Ibidem

⁶¹⁸ CJUE, 26 juillet 2017, avis 1/15.

⁶¹⁹ CJCE, 30 mai 2006, Parlement c/ Conseil, préc.

⁶²⁰ S. CASTELLIER, « Compagnies aériennes des pays du Golfe, l'art du copier-voler », *Orient XXI*, 12 octobre 2021, en ligne à URL : <https://orientxxi.info/magazine/compagnies-des-pays-du-golfe-l-art-du-copier-voler,5082> consulté le 22 août 2024.

⁶²¹ Conseil de l'Union européenne, « Prévention du terrorisme et de l'extrémisme violent et lutte contre ces phénomènes: le Conseil adopte des conclusions sur l'action extérieure de l'UE », Communiqué de presse, *Union européenne*, 16 juin 2020.

Ligue, des Commissions spécialisées et le Secrétariat général. Ces pays fondateurs ont été rejoints par le Yémen après la signature du Pacte par ce dernier en mai 1945⁶²².

Avant la signature de ce pacte fondateur, les six États fondateurs de la Ligue avaient adopté, le 7 octobre 1944, un avant-projet de pacte consultatif de la Ligue et du Protocole d'Alexandrie. Par ailleurs, dans une annexe adossée au Pacte, les États fondateurs avaient pris le soin de désigner un représentant arabe pour la Palestine dont la mission était de participer aux travaux du Conseil de la Ligue. Cela étant dit, depuis juin 1976, la Palestine, représentée par l'Organisation de Libération de la Palestine (O.L.P) a été considérée comme un membre à part entière⁶²³.

Aujourd'hui, la Ligue des États arabes regroupe vingt-deux États repartis sur les continents asiatique et africain (l'Algérie, l'Arabie saoudite, le Bahreïn, les Iles des Comores, Djibouti, l'Égypte, les Émirats arabes unis, l'Irak, la Jordanie, le Koweït, le Liban, la Libye, le Maroc, la Mauritanie, le Sultanat d'Oman, la Palestine, le Qatar, la Somalie, le Soudan, la Syrie, la Tunisie, et le Yémen). Elle couvre ainsi une grande partie du Proche et Moyen-Orient et le Nord de l'Afrique⁶²⁴, allant des côtes atlantiques de la Mauritanie et du Maroc, au Sultanat d'Oman qui borde la mer d'Arabie, regroupant une population globale dépassant les 440 millions d'habitants vivant sur plus 13 millions de km².

Le Pacte de la Ligue des États arabes ne fait pas mention aux droits de l'Homme alors qu'il a été signé à une période où l'on parlait surtout de l'indépendance des États et de « l'opinion publique arabe » dans ces pays concernés⁶²⁵. Certains auteurs arabes, dont Mohamed Amin Al-Midani, ont tenté de justifier cette absence par les « circonstances difficiles » de l'époque ou par le peu d'intérêt pour cette problématique dans la culture juridique arabe d'alors⁶²⁶. Pourtant, cette question était déjà considérée par d'autres organisations. Al-Midani rappelle ainsi que la Charte de l'Organisation des États américains contenait des dispositions faisant référence aux droits de l'Homme, bien qu'elles aient été adoptées en 1948, soit trois ans après l'adoption du Pacte de la Ligue des États arabe⁶²⁷. L'absence de considération des droits de

⁶²² M.A. AL-MIDANI, « La ligue des États arabes et les droits de l'Homme », *Scienza & Politica*, juin 2002, en ligne à URL : <https://doi.org/10.6092/issn.1825-9618/2892> consulté en ligne le 13 mars 2023.

⁶²³ Ibidem

⁶²⁴ M. TERRACOL, « Quel est le rôle de la Ligue arabe ? », *GEO*, 5 octobre 2022, en ligne à URL : <https://www.geo.fr/geopolitique/quel-est-le-role-de-la-ligue-arabe-211898> consulté en ligne le 13 mars 2023.

⁶²⁵ Egmont Institute, « Pacte de la Ligue des États Arabes », *Jstor*, 22 mars 1945, en ligne à URL : <https://www.jstor.org/stable/44827318> consulté en ligne le 13 mars 2023.

⁶²⁶ M.A. AL-MIDANI, « La ligue des États arabes et les droits de l'Homme », *Scienza & Politica*, juin 2002, en ligne à URL : <https://doi.org/10.6092/issn.1825-9618/2892> consulté en ligne le 13 mars 2023. Lire également. B. BOUTROS-GHALI, « La crise de la Ligue arabe », *Annuaire français de droit international*, 1968, p. 87.

⁶²⁷ Ibidem

l'Homme ne semble donc pas être en lien avec une époque, celui de la décolonisation, mais plutôt d'un rapport à des concepts venant d'une culture juridique différente. Pour Al-Midani, il s'agit d'une « crise » de la Ligue et d'un « retard par rapport à d'autres continents » comme l'Afrique⁶²⁸.

Toutefois, la promotion et la protection des droits de l'Homme ne sont pas restées longtemps absentes de l'agenda de la Ligue des États arabes. En effet, le Conseil la Ligue a créé, à travers sa résolution 2443 (XLVIII), le 3 septembre 1968, la Commission permanente arabe pour les droits de l'Homme. Par ailleurs, avant même la création de cette commission, le Conseil s'était investi sur des questions relatives aux droits de l'Homme. Ainsi, il avait accepté l'invitation lancée par les Nations Unies pour participer à l'année internationale des droits de l'Homme. Par la résolution 2259 (XLVI), le Conseil a créé, le 12 septembre 1966, un Comité *ad hoc*, au sein du Secrétariat général, pour la formulation d'un programme de célébration de cette année onusienne. Puis, la résolution 2304 (XLVII) du Conseil de la Ligue, du 18 mars 1967, a créé un deuxième comité « d'orientation » qui a été chargé de coopérer avec le premier afin de mettre en place les modalités de participation de la Ligue à cette célébration⁶²⁹.

Conçue comme une commission de « promotion » des droits de l'Homme, cette instance n'a cependant aucun pouvoir de sanction. Il s'agit d'une Commission dont les fonctions résident dans « l'information et la coordination ». Chaque État de la Ligue dispose d'une voix lors de votes au sein de cette Commission. Jusqu'à aujourd'hui, elle a tenu plusieurs réunions et participé à divers événements donnés par des organisations régionales ou internationales. Toutefois, Mohamed Amin Al-Madani rappelle que cette dernière a choisi de limiter ses activités « aux violations des droits de l'Homme dans les territoires occupés par Israël... »⁶³⁰.

En outre, Zoulikha Hattab⁶³¹ souligne que le monde arabe souffre de plusieurs lacunes dont l'une des principales est l'absence de garanties des libertés. Le rapport sur le développement humain arabe de 2016, révèle un retard dû à la persistance des conflits qui sont en « perpétuelle augmentation »⁶³². Le rapport note également que le développement humain se concentre avant tout sur les libertés individuelles : il s'agit de permettre à chaque personne de

⁶²⁸ Ibid.

⁶²⁹ Ibidem

⁶³⁰ Ibid.

⁶³¹ Z. HATTAB, « Droits et libertés fondamentaux en droit musulman : le paradoxe de l'universalité », *Droit*, Université d'Avignon, 2018, en ligne à URL : <https://theses.hal.science/tel-02073604/document> consulté en ligne le 13 mars 2023.

⁶³² Arab Human Development Report, Youth and the Prospects for Human Development in a Changing Reality, UNDP, 2016.

réaliser son potentiel complet, et non seulement à une minorité ou à la majorité, mais à toutes les personnes, partout dans le monde, aujourd'hui et à l'avenir. C'est ce principe d'universalité qui distingue le paradigme du développement humain. Or, les lacunes dans ce domaine dans le monde arabe semblent avoir un impact significatif sur la place de la protection des droits fondamentaux, des droits de l'Homme et des libertés dans cette région du monde.

L'avocat Bechara Tarabay rappelle que les droits fondamentaux, cet ensemble de droits et de libertés essentielles pour l'individu que doivent assurer l'État de droit et la démocratie, souffrent selon les mots d'Antonio Guterres, le Secrétaire Général des Nations Unies, d'une « maladie » qui se propage du Nord au Sud, et de l'Est à l'Ouest, en dévalorisant la protection des droits et des libertés et en favorisant les atteintes aux droits des réfugiés et des migrants, la traite des êtres humains ainsi que la discrimination des minorités et des communautés autochtones⁶³³. Pour Bechara Tarabay, les citoyens des pays arabes se trouvent ainsi dans un système juridique où les droits et libertés des citoyens sont affaiblis par « un processus de réduction » de l'individu au groupe auquel il appartient, puis ce même groupe est réduit au parti ou à la dynastie qui « s'arroge le pouvoir de le représenter » et cette réduction va jusqu'à l'exclusion de toute aspiration de l'individu arabe à la reconnaissance de ses droits fondamentaux⁶³⁴. C'est dans ce contexte juridique et politique que s'inscrivent les enjeux de la protection des droits fondamentaux dont font partie la protection des données à caractère personnel et la protection de la vie privée.

§ 2 – La protection des données personnelles dans les pays de la Ligue arabe

Les pays du Moyen-Orient ont des plans ambitieux en matière de croissance économique, de développement des nouvelles technologies et de création d'un environnement propice à l'innovation au cours des dix à vingt prochaines années⁶³⁵. Tous les pays arabes, et autres pays orientaux ont adopté de nouvelles lois sur la protection des données à caractère personnel en affinant ou élargissant la portée des législations existantes sur les nouvelles technologies de l'information. Néanmoins, le panorama régional n'est pas uniforme. Il existe différentes approches, différents niveaux de maturité en matière de protection des données, avec une application variable et de nombreux défis.

⁶³³ B. TARABAY, « L'opposabilité des droits fondamentaux dans les pays arabes », *Campus international*, 2017, en ligne à URL : <https://avocatcampusinternational.org/accueil-liban/images/presse/Opposabilite-des-droits-fondamentaux-dans-les-pays-arabes.pdf> consulté en ligne le 14 mars 2023.

⁶³⁴ Ibidem

⁶³⁵ S.A. WARREN, "Data Privacy Protection in the Region and Worldwide: Stakes and Challenges", *The MENA Business Law Review*, LexisNexis, 2018.

Le Qatar et les Émirats arabes unis (ci-après les Émirats) sont à l'avant-garde de cette grande ambition⁶³⁶. Le Bahreïn et Oman sont également riches en ressources et entendent se diversifier pour faire face à un monde en mutation. L'Arabie saoudite est aujourd'hui un acteur important avec des projets annoncés d'urbanisation et de diversification de son économie. Un pays non arabe du Moyen-Orient, la Turquie, a quant à lui pu s'aligner sur la protection internationale des données et les normes européennes.

La Turquie sert ainsi de point de référence pour l'ensemble de la région. Le principal texte législatif turc relatif à la protection des données est la loi sur la protection des données personnelles n° 6698 du 7 avril 2016. Cette législation est principalement basée sur la directive européenne 95/46/CE. À ce jour, le législateur turc a adopté plusieurs règlements pour mettre en œuvre divers aspects de la loi⁶³⁷. Cependant, avant même l'entrée en vigueur de cette législation, les citoyennes et citoyens turcs avaient, en vertu de l'article 20 de la Constitution turque, les droits suivants en matière de protection des données à caractère personnel : demander la protection de leurs données personnelles ; être informés des données personnelles détenues à leur sujet ; accéder, supprimer et/ou corriger ces données ; être informés si leurs données sont utilisées conformément à la finalité pour laquelle le consentement a été donné.

Le Qatar a voté la loi n° 13 de 2016 relative à la protection de données à caractère personnel pour protéger les données de ses citoyens. Ce faisant, le Qatar est devenu le premier État membre du Conseil de coopération du Golfe (CCG) à promulguer une loi sur la protection des données personnelles. Le ministère des Transports et des Communications a été chargé de faire appliquer la loi. Au Qatar, toute organisation impliquée dans le traitement de données personnelles doit adhérer aux principes de transparence, d'équité et de respect de la dignité humaine. En outre, des mesures techniques et organisationnelles adéquates doivent être mises en place pour garantir la sécurité des données personnelles. Cette législation prévoit des sanctions financières en cas de non-conformité ou de violation de la législation⁶³⁸ pouvant aller jusqu'à un maximum de 5 millions de riyals qataris⁶³⁹.

Le 1^{er} août 2019, la loi n° 30 de 2018 sur la protection des données personnelles est entrée en vigueur dans le Royaume de Bahreïn. Inspirée de la législation européenne sur la protection

⁶³⁶ Ibidem

⁶³⁷ Briefing, "Data Protection Is Trending In The Middle East", *Privacy Solved*, en ligne à URL: <https://www.privacysolved.com/data-protection-is-trending-in-the-middle-east/> consulté en ligne le 6 mars 2023.

⁶³⁸ Qatar, *Data Guidance*, 2022, en ligne à URL : <https://www.dataguidance.com/jurisdiction/qatar-financial-centre> consulté en ligne le 6 mars 2023.

⁶³⁹ 5 millions de riyals qataris équivalent en 2024 à 1,2 million d'euros.

des données, il s'agit de la deuxième loi nationale de la région du Golfe à traiter directement du droit à la protection des données personnelles. Celle-ci impose aux entreprises qui collectent des données personnelles des obligations dans la manière dont elles les utilisent et les sécurisent⁶⁴⁰. Les sanctions vont plus loin que celles prévues par le RGPD de l'UE puisque des dispositions prévoient des peines de prison pouvant aller jusqu'à 1 an⁶⁴¹. Par ailleurs, cette loi prévoit des exigences supplémentaires pour les organisations dont celles de mettre à jour, mensuellement, leurs registres de traitement des données.

En novembre 2021, les Émirats arabes unis ont voté la loi fédérale n° 45 qui fixe des normes plus strictes en matière de confidentialité et de protection des données à caractère personnel et sensibilise davantage à l'importance du respect de la protection des données. Une législation dans la zone franche du Dubaï International Financial Centre (ci-après DIFC) est également entrée en vigueur. La loi DIFC n° 5 de 2020 du 1^{er} juillet 2020 est applicable depuis le 1^{er} octobre 2020. Elle s'applique à toutes les entités enregistrées au DIFC et vise à protéger les données des personnes traitées par des organisations inscrites à celui-ci. Le non-respect de la loi peut entraîner des amendes. Influencée par le RGPD de l'UE, la loi reprend les standards européens en matière de protection des données⁶⁴².

La loi saoudienne sur la protection des données personnelles a quant à elle été publiée le 16 septembre 2021 dans le but de protéger et de fournir des directives sur le traitement des données personnelles au sein du Royaume d'Arabie saoudite. La loi s'applique à toutes les organisations qui opèrent ou font des affaires en Arabie saoudite. Cette loi a officiellement été applicable 180 jours après son annonce, soit le 23 mars 2022. Cependant, il a existé un délai de grâce d'un an que les responsables de traitement de données pouvaient utiliser pour se mettre en conformité. Cette législation a été complétée par des règlements d'application qui devraient clarifier davantage de nombreuses dispositions. Le règlement exécutif a été publié le 10 mars 2022. Si une organisation ne protège pas les données personnelles et ne se conforme pas à la loi dans un délai d'un an, les amendes peuvent atteindre jusqu'à 5 millions de riyals saoudiens et des peines de prison jusqu'à 2 ans⁶⁴³.

⁶⁴⁰ DLAIPER, "Bahrain", *Data protection law of the world*, 2023, en ligne à URL : <https://www.dlapiperdataprotection.com/index.html?t=law&c=BH> consulté en ligne le 6 mars 2023.

⁶⁴¹ Au sein de l'Union européenne, les sanctions pénales relèvent de la compétence des États membres. Bien que le RGPD ne prévoit pas de sanctions pénales, la législation nationale, comme le code pénal en France, établit des sanctions en matière de protection des données personnelles. C'est le cas de l'article 226-16 qui prévoit cinq ans d'emprisonnement.

⁶⁴² M. WHITE, P. MENNIE, O. SYKES, R. CHUDZYNSKI, "Data privacy handbook for the United Arab Emirates", PWC, 2021.

⁶⁴³ A. LECLAIRE, « La 'personal data protection law' d'Arabie saoudite », *Village de la justice*, 1^{er} août 2022, en ligne à URL : <https://www.village-justice.com/articles/personal-data-protection-law-arabie->

L'Égypte a voté, en juillet 2020, une loi sur la protection des données personnelles qui énonce de multiples droits à destination des individus en la matière. Conformément à cette loi, les données personnelles ne doivent être collectées qu'à des fins légitimes spécifiques et ne doivent pas être conservées plus longtemps que nécessaire. Les organisations peuvent avoir besoin d'acquiescer une licence pour traiter à la fois les données personnelles et les données personnelles sensibles. En outre, les organisations impliquées dans le traitement des informations personnelles doivent nommer un délégué à la protection des données responsable de l'application de cette loi au sein de l'organisation. La loi sur la protection des données personnelles prévoit des amendes administratives et des sanctions pénales en cas de non-respect pouvant aller jusqu'à un maximum de 5 millions de livres égyptiennes ou une peine d'emprisonnement potentielle de plus de six mois⁶⁴⁴.

En février 2022, le Sultanat d'Oman a publié la loi sur la protection des données personnelles qui fixe des normes strictes en matière de confidentialité et de protection des données et renforce la sensibilisation à l'importance du respect de la protection des données à caractère personnel. La loi, entrée en vigueur le 13 février 2023, invite les organisations à se conformer aux nouvelles exigences légales⁶⁴⁵.

Le Koweït n'a pas de législation spécifique sur la protection des données à caractère personnel. Toutefois, l'Autorité de régulation des communications et des télécommunications a publié la décision n° 42 de 2021 portant règlement sur la protection des données à caractère personnel imposant des obligations en la matière aux fournisseurs de services de télécommunication et aux secteurs industriels connexes⁶⁴⁶.

Le règlement définit des lignes directrices détaillées pour la collecte, le stockage, le traitement et le transfert de données par les prestataires de services du secteur privé et du secteur public. La partie la plus intéressante de ce document est la définition large de « fournisseur de services »⁶⁴⁷ qui a été retenue, s'étendant des fournisseurs de services de télécommunications traditionnels à toute personne qui exploite un site web, une application intelligente, un service d'informatique en nuage, qui collecte ou traite des données personnelles ou dirige une autre

[saoudite,43326.html#:~:text=A%20l'instar%20de%20quelques,vigueur%20le%2017%20mars%202023.](#)
consulté en ligne le 6 mars 2023.

⁶⁴⁴ Egypt, *Data Guidance*, 2022, en ligne à URL : <https://www.dataguidance.com/notes/egypt-data-protection-overview> consulté en ligne le 6 mars 2023.

⁶⁴⁵ Oman, *Data Guidance*, 2022, en ligne à URL : <https://www.dataguidance.com/news/oman-data-protection-law-comes-force#:~:text=Royal%20Decree%20No.,1429%2C%20on%2013%20February%202022>, consulté en ligne le 6 mars 2023.

⁶⁴⁶ DLA Piper, "Kuwait", *Data protection law of the world*, 22 décembre 2022, en ligne à URL : <https://www.dlapiperdataprotection.com/index.html?t=law&c=KW>, consulté en ligne le 7 mars 2023.

⁶⁴⁷ Ibidem

partie de le faire en son nom et par l'intermédiaire de centres d'information détenus ou utilisés par eux directement ou indirectement.

Les exclusions des obligations, prévues par le règlement, concernent la collecte et le traitement de données personnelles par un individu ou les agences sécuritaires aux fins de contrôle des crimes et de mise en œuvre des mesures de sécurité de l'État. Cela s'ajoute aux obligations issues de la loi n° 20 de 2014 – loi sur le commerce électronique – qui exige que les données des clients relatives aux affaires de position, au statut personnel, à l'état de santé, à certaines informations financières et à d'autres informations personnelles soient conservées de manière privée et confidentielle par le bénéficiaire et ses employés. Ces données ne peuvent être divulguées sans le consentement du client ou une décision de justice.

Au Liban, en vertu de la loi n° 81 du 10 octobre 2018 sur les transactions électroniques et les données personnelles, les responsables de traitement qui opèrent dans le pays sont responsables du respect des principes de protection des données, dont le principe de limitation des finalités considérant qu'un traitement doit être licite, sûr, spécifique et transparent.

La Jordanie a publié sa loi n° 24 sur la protection des données à caractère personnel le 17 septembre 2023 après avoir préparé ce nouveau cadre juridique pour plusieurs mois⁶⁴⁸, qui lui permet d'être sur le même plan avec les autres législations votées dans les différents pays de la ligue arabe.

L'Irak, l'Iran, la Palestine, la Syrie et le Yémen ne disposent pas de lois nationales ou n'ont pas mis en œuvre de projets de loi sur la protection des données à caractère personnel.

Ces changements de politique visent à mettre en avant les droits individuels, moins politiques qu'économiques, et à renforcer la confiance dans les nouvelles technologies dans une région où s'accroissent les flux de données internationaux et régionaux. La protection des données à caractère personnel est devenue une priorité au Moyen-Orient, en raison des investissements substantiels de la région dans les domaines des données, de la technologie, de l'automatisation, des villes intelligentes et de l'innovation scientifique. Cependant, l'efficacité de ces législations reste encore à démontrer⁶⁴⁹.

Dans les pays du Maghreb, la tradition juridique est plus proche des pays européens avec qui ces États partagent une proximité culturelle. Au Maroc tout d'abord, la loi régissant la vie

⁶⁴⁸ DLAPIPER, "Jordan", *Data protection law of the world*, 19 janvier 2023, en ligne à URL : <https://www.dlapiperdataprotection.com/index.html?t=law&c=JO&c2=>, consulté en ligne le 7 mars 2023.

⁶⁴⁹ M. WHITE, P. MENNIE, O. SYKES, R. CHUDZYNKSI, *Data privacy handbook for the United Arab Emirates*, PWC, 2021.

privée et la protection des données est la loi n° 09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Ce texte vise, d'une part, à assurer une protection efficace des particuliers contre les abus d'utilisation des données de nature à porter atteinte à leur vie privée et, d'autre part, à harmoniser le système marocain de protection des données personnelles avec celui de ses partenaires, notamment européens. En outre, cette législation a institué une Commission nationale de protection des données personnelles (CNDP)⁶⁵⁰.

La loi sur la protection des données régit le traitement automatique et certains traitements manuels des données personnelles et des données personnelles sensibles. Par traitement de données à caractère personnel, la législation entend toute opération ou ensemble d'opérations effectuées par des moyens, automatiques ou non, et faisant partie d'un fichier. La loi sur la protection des données régit la collecte et le traitement des données personnelles des personnes physiques, au Maroc, et ne protège pas les personnes morales telles que les sociétés à responsabilité limitée et les sociétés à responsabilité illimitée. La CNDP est responsable de l'application de cette loi sur la protection des données.

L'Algérie dispose de la loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel. L'article 1^{er} de cette législation a pour objet de fixer des règles de protection des données personnelles qui se traduisent par la consécration de nouveaux principes, de nouveaux droits et la mise en place de nombreuses obligations. Cette dynamique a permis, en 2020, la constitutionnalisation du principe de protection des données à caractère personnel à travers une nouvelle disposition introduite dans la Constitution algérienne. Le principe de finalité est considéré comme la pierre angulaire de cette législation. Ainsi, pour être licite, un traitement de données à caractère personnel doit être assorti d'une finalité⁶⁵¹.

La Tunisie a été pionnière dans la région du Maghreb depuis 2002 en matière de protection des données personnelles avec la loi n° 2004-63 du 27 juillet 2004⁶⁵² portant sur la protection

⁶⁵⁰ Royaume du Maroc, Direction générale de la sécurité des systèmes d'information, Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, en ligne à URL : <https://www.dgssi.gov.ma/fr/content/loi-09-08-relative-la-protection-des-personnes-physiques-l-egard-du-traitement-des-donnees-caractere-personnel.html#:~:text=Cette%20loi%20vise%20C3%A0%20assurer,de%20ses%20partenaires%20notamment%20europ%C3%A9ens.>, consulté en ligne le 7 mars 2023.

⁶⁵¹ R. ARADJI, « Loi n°18-07 : Protection des données personnelles », Groupement Algérien des Acteurs du Numérique, 2020 en ligne à URL : <https://www.gaan.dz/articles-divers/loi-n18-07--protection-des-donnees-personnelles-page-115653> consulté en ligne le 8 mars 2023.

⁶⁵² Loi organique n° 2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel. Voir également. DLAPIPER, "Tunisia", Data protection law of the world, 22 août 2024, en ligne à URL :

des données à caractère personnel. Cette loi a été suivie en 2014 par la consécration constitutionnelle de la protection de la vie privée, érigeant ce droit au premier rang des droits et libertés à garantir dans la nouvelle Constitution tunisienne. Par ailleurs, les articles 56, 61 et 75 de la loi organique n° 2015-26 du 7 août 2015 relative à la lutte contre le terrorisme et à l'interdiction du blanchiment d'argent traitent du sujet des données personnelles et des cas dans lesquels l'utilisation des données personnelles est autorisée. Puis, le 1^{er} novembre 2017, la Tunisie est devenue le 51^e État membre de la Convention 108 du Conseil de l'Europe. En mars 2018, elle a présenté au Parlement un nouveau projet de loi sur la protection des données personnelles conforme au RGPD.

En Libye, les articles 12 et 13 de la Constitution de 2011 garantissent le droit à la vie privée des citoyens ainsi que la confidentialité de leurs correspondances, conversations téléphoniques et autres formes de communication, sauf en cas de réquisition autorisée par un mandat judiciaire⁶⁵³. Cependant, l'effectivité de ce droit suscite des interrogations, compte tenu de la situation politique instable qui prévaut dans le pays.

En Mauritanie, cinq ans après la promulgation de la loi informatique et libertés n° 2017-020 du 22 juillet 2017, le Gouvernement a adopté, en février 2022, le règlement portant composition, organisation et fonctionnement de l'Autorité de protection des données. Quelques mois plus tard, les membres de l'Autorité de protection des données ont prêté serment, dont son président⁶⁵⁴.

Les avancées réalisées en matière de protection des données à caractère personnel dans les pays du Maghreb pourraient déboucher sur un futur partenariat euromaghrébin, qui a été envisagé compte tenu des visions convergentes des cultures juridiques⁶⁵⁵. Différents hauts fonctionnaires, universitaires et experts, au Maghreb comme en Europe, ont discuté de ces questions en matière de sécurité et de défense ainsi que de coopération s'agissant de la lutte contre le terrorisme et l'immigration illégale.

Cependant, la sensibilisation aux questions de protection des données à caractère personnel dans ces pays semble surtout provenir des acteurs économiques. Ainsi, au Maroc, des séminaires de sensibilisation ont été organisés dans les milieux bancaires en vue d'améliorer

<https://www.dlapiperdataprotection.com/index.html?c=TN&c2=&go-button=GO&t=law> , consulté en ligne le 22 août 2024.

⁶⁵³ DLA Piper, "Lybie", *Data protection law of the world*, 13 janvier 2023, en ligne à URL : <https://www.dlapiperdataprotection.com/index.html?t=law&c=LY&c2=> consulté en ligne le 8 mars 2023.

⁶⁵⁴ A. SYLLA, « Recent developments in African data protection laws - Outlook for 2023 », *Hogan Lovells*, février 2023, en ligne à URL : <https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45> consulté en ligne le 8 mars 2023.

⁶⁵⁵ EUSS, le Maghreb et l'Union européenne : vers un partenariat privilégié ? Seminar report, 25 octobre 2014.

la compréhension des acteurs bancaires et institutionnels en matière de protection des données à caractère personnel. Enfin, notons que la plupart des acteurs économiques autour de la Méditerranée sont concernés par le respect des exigences du RGPD, puisqu'ils opèrent à destination de l'espace européen⁶⁵⁶.

§ 3 – Des accords PNR avec des pays arabes évoqués sans être concrétisés

En principe, ce sont les États qui fixent les conditions de transferts des données des dossiers passagers que les compagnies aériennes doivent respecter pour pouvoir desservir dans le territoire en question⁶⁵⁷. Cela étant dit, afin de réguler ces transferts, l'Organisation de l'aviation civile internationale (OACI) a publié des lignes directrices⁶⁵⁸. En 2013, seulement neuf pays exigeaient l'accès au dossier passager⁶⁵⁹ tandis qu'aujourd'hui plus de 60 pays utilisent les données PNR pour lutter contre le terrorisme et la grande criminalité, dont tous les États de l'Union européenne⁶⁶⁰.

En plus des accords déjà établis avec les États-Unis, le Canada, l'Australie, ainsi que de celui en cours de négociation avec le Japon, les discussions pour un accord entre l'UE et le Mexique sur le transfert de données PNR ont officiellement commencé le 14 juillet 2015. Le mandat pour ces négociations a été donné à la Commission le 23 juin 2015, après des débats préliminaires en session plénière le 15 avril 2015 et en commission des libertés civiles le 4 juin 2015⁶⁶¹.

⁶⁵⁶ Maroc.ma, « M. Jouahri : La protection des données revêt une importance capitale pour Bank Al Maghrib », *Actualité*, 14 Juin 2019.

⁶⁵⁷ Sénat, Justice et affaires intérieures, Texte E 6014, Communication de M. Simon Sutour sur la proposition de directive « Passenger Name Record » (PNR européen), COM(2011) 32 final, Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, COM(2011) 32 final du 2 février 2011, Examen dans le cadre de l'article 88-4 de la Constitution, texte déposé au Sénat le 9 février 2011, examens : 12 avril 2011 (commission des affaires européennes), 4 février 2015 (commission des affaires européennes), propositions de résolution n° 427 (2010-2011) et n° 281 (2014-2015).

⁶⁵⁸ OACI, Lignes directrices sur les données des dossiers passagers (PNR), Doc 9944, 2010. Par exemple, le point 2.6.1 prévoit que les États devraient uniquement demander des données PNR aux exploitants d'aéronefs opérant des vols vers ou depuis leurs aéroports, ou en transit, y compris en cas de déroutement, tout en acceptant une fourniture limitée de ces données pour les déroutements imprévus.

⁶⁵⁹ IATA, Annual review, 2013, en ligne à URL : <https://www.iata.org/contentassets/c81222d96c9a4e0bb4ff6ced0126f0bb/iata-annual-review-2013-en.pdf> consulté en ligne le 23 mars 2023.

⁶⁶⁰ Confédération suisse, « Consultation concernant la loi sur les données relatives aux passagers aériens, LDPa », Office fédéral de la police fedpol, 2022, en ligne à URL : <https://www.fedpol.admin.ch/fedpol/fr/home/polizei-zusammenarbeit/international/flugpassagierdaten.html> consulté en ligne le 23 mars 2023.

⁶⁶¹ Parlement européen, « Accords PNR avec des pays tiers », 1 juin 2016, en ligne à URL : <https://www.europarl.europa.eu/news/fr/press-room/20150123BKG12902/directive-sur-les-donnees-des-dossiers-passagers-de-l-ue-donnees-pnr-aperçu/10/accords-pnr-avec-des-pays-tiers> consulté le 22 août 2024. À ce jour, il n'y a eu aucune avancée sur le projet d'accord EU-Mexique.

Toutefois, certains États, comme le Qatar, exigent désormais des compagnies aériennes européennes la communication de leurs données PNR. Le 31 mars 2021, Qatar Airways, société par actions qatarienne⁶⁶², a publié sa politique aérienne vis-à-vis des tiers prévoyant une série de dispositions et de conditions relatives aux bagages, aux changements de vol, aux sièges mais aussi au traitement des données à caractère personnel.

Par exemple, l'article 10.3 de ces conditions générales prévoit que l'agent qui procède à l'enregistrement des passagers doit fournir, à Qatar Airways, des informations PNR complètes et exactes, y compris toutes les informations de contact telles que les numéros de téléphone et les adresses électroniques fournies par les clients, ainsi que toute autre information requise par le gouvernement et les autorités chargées de l'application de la loi. Ce traitement n'est pas prévu sans un encadrement juridique puisque ces conditions rappellent que Qatar Airways traitera toutes les informations des dossiers passagers reçues conformément à sa politique de confidentialité et à toutes les lois applicables.

Or, la dernière Coupe du monde au Qatar a révélé de supposées violations des règles en matière de respect de la protection des données à caractère personnel au Qatar⁶⁶³ que le BfDI - l'autorité allemande de protection des données - a dénoncé. C'est le cas pour les applications obligatoires que devaient télécharger les visiteurs dans le pays pour assister à la Coupe du monde 2022. L'autorité allemande a annoncé qu'elle avait été en mesure de déterminer que le traitement des données des deux applications qatariennes allait probablement beaucoup plus loin que ne l'indiquaient les descriptions des avis de protection des données et des finalités de traitement dans les fiches des applications. Ce cas montre l'actuel et réel niveau de protection des données personnelles au Qatar, qui n'est pas aussi effectif que pourrait le suggérer la législation en place. En effet, comme il a été rappelé ci-dessus, l'application effective des droits fondamentaux dans les pays arabes n'a pas encore été atteinte car la consolidation de l'État de droit y est encore fragile.

Les compagnies aériennes, comme Qatar Airways, manquent des garanties offertes par un cadre juridique sûr comme peuvent en bénéficier les voyageurs et les transporteurs aériens européens. Les accords PNR permettent d'assurer aux acteurs un niveau de protection de données satisfaisant. En l'absence d'accord, ces acteurs se trouveront exposés soit à se mettre

⁶⁶² Qatar Airways, "Qatar Airways Partner Agency Policies", *Airline Policy (COM-100)*, 31 mars 2021, en ligne à URL : https://www.qatarairways.com/content/dam/tradepartners/pdf-files/QAPAP_Qatar-Airways-Partner-Agency-Policies.pdf consulté en ligne le 23 mars 2023.

⁶⁶³ BfDI, "Instructions for using the Ehteraz and Hayya apps", 15 novembre 2022, en ligne à URL : https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2022/22_Etheraz-Hayya.html consulté en ligne le 22 mars 2023.

en contradiction avec le droit applicable s'ils transmettent les données, soit à des mesures de restriction de vols de la part d'États tiers⁶⁶⁴.

L'autre point que le CEPD avait mis en avant est la question de la réciprocité dans les accords bilatéraux d'échange de données des dossiers passagers. En effet, ce dernier a relevé que « la réciprocité pourrait conduire à communiquer des données à caractère personnel à des pays dans lesquels aucune garantie ne peut être donnée en termes de normes démocratiques et de niveau adéquat de protection des données »⁶⁶⁵. C'est pourquoi, l'adéquation des standards de niveau de protection, également présente dans le cadre des échanges de données hors Union européenne dans le RGPD, est un sujet sensible car certains États, comme ceux de la Ligue arabe, la Chine ou la Russie, ne disposent pas des mêmes standards de protection que l'Union européenne. La Chine, par exemple, prévoit la possibilité de demander aux usagers des transports aériens de fournir leurs données personnelles, dont les données PNR, aux autorités gouvernementales et aux organismes de réglementation à des fins d'immigration, de douane et de sécurité des frontières⁶⁶⁶.

Précisément, en Chine, la Personal Information Protection Law, votée le 1^{er} novembre 2021, régit la collecte et le traitement des données à caractère personnel. Cette législation est vue comme « nationaliste et protectionniste », à l'image de la politique actuelle de la Chine, dans un contexte de politique intérieure où « la criminalité de l'information » est en forte croissance⁶⁶⁷. Ce qui a pu être présenté comme l'équivalent du RGPD n'a pas été analysé comme tel par Olivier Dufour et Marie-Anne Frison-Roche⁶⁶⁸ qui rappellent qu'en Chine, c'est l'État qui gère la connaissance de l'information et dispose d'un accès discrétionnaire à celle-ci. En effet, cette législation chinoise précise que l'impossibilité de collecter et traiter des données personnelles s'impose aux entreprises mais pas à l'État. Ainsi, le pouvoir

⁶⁶⁴ S. SUTOUR et Y. DETRAIGNE, « Rapport n° 401 : La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives », *Sénat*, Commission des lois, 13 mai 2009, en ligne à URL : <http://www.senat.fr/ue/pac/E6014.html> consulté en ligne le 23 mars 2023.

⁶⁶⁵ CEPD, « Avis du Contrôleur européen de la protection des données du 1^{er} mai 2008 sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives », JOUE n° C 110, 1^{er} mai 2008.

⁶⁶⁶ China Airlines, « Privacy Protection », 31 mai 2022, en ligne à URL : <https://www.china-airlines.com/us/en/terms-and-conditions/privacy-protection> consulté en ligne le 22 mars 2023.

⁶⁶⁷ P. CADIO, F. NGUYEN, « RGPD/PIPL : superposition et empiètement des réglementations sur la protection des données personnelles des citoyens d'Europe et de Chine », *LpaLaw*, Option Finance n° 1662, 4 juillet 2022, en ligne à URL : <https://www.lpalaw.com/wp-content/uploads/2022/07/2022.07-Option-Finance-PIPL-RGPD.pdf> consulté en ligne le 26 mars 2023.

⁶⁶⁸ O. DUFOUR, M-A FRISON-ROCHE, « La nouvelle loi de protection des données en Chine est un 'anti-RGPD' », *Actu-juridique*, 2 septembre 2021, en ligne à URL : <https://www.actu-juridique.fr/ntic-medias-presse/la-nouvelle-loi-de-protection-des-donnees-en-chine-est-un-anti-rgpd/> consulté en ligne le 26 mars 2023.

politique chinois arrive ainsi à limiter la montée en puissance des grandes entreprises technologies chinoise pouvant rivaliser en puissance avec l'État⁶⁶⁹.

Cette situation conduit à une inadéquation de la Chine avec les standards européens relatifs à la protection des données personnelles ayant pour conséquence un risque de faire naître des cas dans lesquels des données des passagers aériens de citoyens européens sans protection et en état de vulnérabilité soient transmises à des pays tiers, exposant ainsi le citoyen européen à une violation de son droit à la vie privée et de son droit à la protection des données à caractère personnel défendus par le Charte des droits fondamentaux de l'Union européenne. Par conséquent, le CEPD « estime qu'il est de la plus haute importance que les conditions de la transmission des données PNR à des pays tiers soient cohérentes et soumises à un niveau harmonisé de protection »⁶⁷⁰. Ce risque d'exposition à un droit, peu protecteur, comme c'est le cas dans les pays de la Ligue arabe, explique en partie la raison pour laquelle, jusqu'à aujourd'hui, il n'y a pas eu d'accord PNR entre l'Union européenne et un pays de la Ligue arabe.

Section 2 – La limitation des droits fondamentaux au nom de la sécurité publique

Depuis 2009, l'Union européenne dispose d'une Charte des droits fondamentaux qui répond à deux principaux objectifs. Le premier est d'offrir des références claires et fortes, compréhensibles pour chaque citoyen européen. C'est pourquoi la Charte, d'une part, regroupe des droits existants prévus dans la Convention européenne de sauvegarde des droits de l'Homme, la Charte sociale européenne et d'autres textes et, d'autre part, enrichit la liste des droits de l'Homme protégés en Europe en considérant de nouveaux domaines dont la protection des données à caractère personnel. Le second objectif est la protection des droits fondamentaux. En effet, aucun inventaire détaillé de ces droits n'a été incorporé dans un traité avant la Charte ; la seule protection dont disposaient les Européens auparavant étaient fournie par l'article 6 TUE indiquant que « l'Union respecte les droits fondamentaux » et la jurisprudence de la CJUE, notamment dans son avis 1/15⁶⁷¹.

⁶⁶⁹ Sur la relation stratégique entre l'Union européenne et la Chine. Lire J-C. BEAUJOUR, « La nouvelle donne internationale et les opportunités de coopération stratégique UE/Chine », *Revue Défense Nationale*, Revue n° 838 Mars 2021, p. 83-89.

⁶⁷⁰ CEPD, « Avis du Contrôleur européen de la protection des données du 1^{er} mai 2008 sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives », JOUE n° C 110, 1^{er} mai 2008.

⁶⁷¹ P. GRECIANO, « La jurisprudence de la Cour de justice de l'Union européenne », *Revue française de linguistique appliquée*, 2014, pp. 59-70. Voir aussi. J. TRICOT, « Droit et jurisprudence de l'UE », *Revue de science criminelle et de droit pénal comparé*, 2018, pp. 203-228.

L'article 52 § 1 de la Charte des droits fondamentaux prévoit que « toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui »⁶⁷². Les limitations aux droits fondamentaux sont possibles en satisfaisant les conditions énumérées dont celles prévues par « la loi ». Cette disposition se lit à l'aune de l'article 8 de la même Charte qui considère que le traitement des données à caractère personnel doit être effectué sur « la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi »⁶⁷³. Or, le transfert des données PNR n'est pas conditionné au consentement des voyageurs, comme l'a rappelé la Cour dans le point 144 de son avis 1/15 du 27 juillet 2017⁶⁷⁴.

Le droit français définit la sécurité à l'article L. 111-1 du code de la sécurité intérieure comme « un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives » sachant que l'État « a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre public, à la protection des personnes et des biens »⁶⁷⁵. La notion d'ordre public est importante à définir puisqu'elle implique « la préservation du bon ordre, de la sûreté, de la sécurité et de la salubrité publique et plus récemment du respect de la dignité de la personne humaine »⁶⁷⁶.

Dans son arrêt Royer⁶⁷⁷, la Cour de justice a assimilé les deux notions, examinant une mesure d'éloignement prise par un État au regard d'un comportement menaçant « l'ordre et la sécurité publics », ce sur le fondement du traité sur les Communautés européennes et de la directive européenne n° 64/ 221⁶⁷⁸. Toutefois, la directive 2004/38 du Parlement européen et du Conseil relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres⁶⁷⁹ impose de distinguer les deux notions. En effet, dans son article 28 paragraphe 3, la directive prévoyait une protection

⁶⁷² Charte des droits fondamentaux de l'Union européenne, article 52 § 1.

⁶⁷³ Charte des droits fondamentaux de l'Union européenne, article 8.

⁶⁷⁴ CJUE, 26 juillet 2017, avis 1/15, Point 144.

⁶⁷⁵ Code de la sécurité intérieure, Article L. 111-1.

⁶⁷⁶ « Ordre public », *Droit administratif*, Dalloz, septembre 2021.

⁶⁷⁷ CJCE, 8 avr. 1976, Royer, aff. C-48/75.

⁶⁷⁸ J-D MOUTON, « Ordre public, sécurité publique », *Droit de séjour, Répertoire de droit européen*, septembre 2022.

⁶⁷⁹ Directive 2004/38 du Parlement européen et du Conseil relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, 2004.

renforcée contre une décision d'éloignement à l'encontre des citoyens de l'Union qui ont résidé au cours des dix années précédentes dans l'État membre d'accueil, ou des mineurs, « sauf si la décision est fondée sur des motifs graves de sécurité publique définis par les États membres ».

L'article 31-2 relatif aux garanties procédurales prévoit qu'une mesure d'éloignement ne peut avoir d'effet qu'après ordonnance de référé, sauf « lorsque la décision d'éloignement est fondée sur des raisons impérieuses de sécurité publique prévues à l'article 28-3 ». Pour J.-D. Mouton, cette formulation n'implique pas que les États disposent d'un pouvoir discrétionnaire illimité pour déterminer ce qui constitue une menace pour la sécurité publique. Cependant, elle a conduit la Cour à préciser les contours de cette notion dans le cadre de son pouvoir de révision des concepts d'ordre public et de sécurité publique.⁶⁸⁰

La lutte contre certains crimes est susceptible de constituer une raison impérieuse de sécurité publique⁶⁸¹. Dans ce contexte, les juges de Luxembourg ont considéré qu'une mesure d'éloignement peut être justifiée si les infractions pénales présentent des caractéristiques particulièrement graves et que le comportement de la personne concernée représente une menace grave, réelle et actuelle pour un intérêt fondamental de la société ou de l'État membre d'accueil⁶⁸². La menace à l'intérêt fondamental de l'État ou de la société semble être ce qui caractérise fondamentalement la sécurité publique. Cette préoccupation exprimée reflète la vigilance préconisée par la doctrine : c'est cet argument sécuritaire qui sera plus tard invoquée pour justifier les restrictions des droits fondamentaux dans le cadre du système PNR.

Dans son avis du 27 juillet 2017 précité portant sur l'accord PNR conclu entre le Canada et l'Union européenne, le juge européen a été amené à vérifier que les limitations aux droits fondamentaux du passager aérien étaient issues d'un accord effectivement fondé sur une mesure légale (sous-section 1) et poursuivant un objectif d'intérêt général (sous-section 2). Cela n'a pas empêché la Cour de considérer en l'espèce que la limitation des droits fondamentaux envisagée était disproportionnée (sous-section 3).

Sous-section 1 – Une limitation fondée sur une interprétation originale de la « loi »

Le fondement de la limitation des droits fondamentaux sur une lecture matérielle de la notion de « loi », au sens de l'article 52 de la Charte, n'avait pas convaincu le Parlement européen qui soutenait « que l'accord international, à défaut de constituer un acte législatif à

⁶⁸⁰ J-D MOUTON, « Ordre public, sécurité publique », Droit de séjour, *Répertoire de droit européen*, septembre 2022.

⁶⁸¹ CJUE, 23 nov. 2010, Tsakouridis, aff. C-145/09.

⁶⁸² J-D MOUTON, « Ordre public, sécurité publique », Droit de séjour, *Répertoire de droit européen*, septembre 2022.

proprement parler, ne relevait pas de la notion de ‘loi’ »⁶⁸³. La Cour a écarté cet argument considérant que la notion de loi doit être lue suivant une approche matérielle et non formelle⁶⁸⁴. En effet, celle-ci a pu considérer qu’un accord international peut être inclus dans la notion de « loi » eu égard notamment à sa prévisibilité et son accessibilité⁶⁸⁵. Dans le droit européen, les accords internationaux sont ratifiés par l’Union et publiés au Journal officiel. Ils forment, selon la formule consacrée par l’arrêt Haegeman⁶⁸⁶, « une partie intégrante » de l’ordre juridique européen à compter de leur entrée en vigueur.

Puis, la Cour a rappelé que la procédure de l’article 218 § 6 du TFUE établit « une symétrie entre la procédure d’adoption des mesures de l’Union sur le plan intérieur et la procédure d’adoption des accords internationaux, afin de garantir que, en rapport avec un domaine donné, le Parlement et le Conseil disposent des mêmes pouvoirs dans le respect de l’équilibre institutionnel prévu par les traités », comme l’a déjà affirmé l’arrêt du 24 juin 2014 Parlement contre Conseil⁶⁸⁷. Ainsi, les juges de Luxembourg ont consacré « l’équivalence entre, d’une part, la procédure d’approbation du Parlement européen pour les accords internationaux portant sur des matières soumises, au plan interne, à la procédure législative ordinaire et d’autre part, la procédure de codécision au plan interne »⁶⁸⁸. La Cour a ainsi indiqué que la procédure législative « ordinaire » n’exclut pas le caractère législatif des autres procédures spécifiques. Elle exprimait par là son attachement aussi bien à l’approche matérielle de la notion de loi qu’à une lecture institutionnelle à même de garantir le respect du principe d’équilibre institutionnel⁶⁸⁹.

Il est intéressant de noter qu’en tant que juridiction interne suprême au sein de l’ordre juridique de l’Union européenne, la Cour de justice réalise un contrôle plus approfondi que la Cour européenne des droits de l’Homme qui se limite à considérer que « c’est au premier chef aux autorités nationales, notamment aux cours et tribunaux, qu’il appartient d’interpréter la législation interne. Il en va de même lorsque le droit interne renvoie à des règles du droit international général ou à des accords internationaux »⁶⁹⁰.

⁶⁸³ V. CORREIA, « À propos de l’avis 1/15 relatif au projet d’accord entre le Canada et l’Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁶⁸⁴ CJUE, 26 juillet 2017, avis 1/15, Point 145.

⁶⁸⁵ Ibidem, point 146.

⁶⁸⁶ CJCE, 30 avril 1974, R. & V. Haegeman c/ État belge, affaire 181-73.

⁶⁸⁷ CJUE, Parlement européen c/ Conseil, affaire C-658-11 relatif au jugement de pirates arrêtés par la force Eunavfor Atalanta, 24 juin 2014.

⁶⁸⁸ V. CORREIA, « À propos de l’avis 1/15 relatif au projet d’accord entre le Canada et l’Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁶⁸⁹ Ibidem

⁶⁹⁰ Ibid.

Sous-section 2 – Une limitation fondée sur un objectif d'intérêt général

Après avoir établi le fondement « légal » des limitations apportées aux droits fondamentaux, les juges de Luxembourg ont constaté que l'accord en question, par le biais de ses limitations, poursuivait un objectif d'intérêt public, plus précisément de sécurité publique : « l'accord envisagé vise, notamment, à garantir la sécurité publique au moyen d'un transfert des données PNR vers le Canada et de l'utilisation de celles-ci dans le cadre de la lutte contre des infractions terroristes et la criminalité transnationale grave »⁶⁹¹. Contrairement à la jurisprudence de l'arrêt *Digital Rights Ireland* où la Cour avait reconnu la pertinence de l'objectif d'intérêt général relatif à la sécurité publique mais sans le privilégier face à l'atteinte aux droits fondamentaux qu'elle jugeait massive et indifférenciée, ici elle a retenu que l'accord permet de satisfaire la protection de la sécurité et de la sûreté publique⁶⁹². C'est aussi une évolution par rapport à sa jurisprudence *Tele2 Sverige* où elle avait identifié cet objectif comme « fondamental » mais ne permettant pas « à lui seul de justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte »⁶⁹³.

Ainsi, pour la Cour, il s'agit d'un « objectif d'intérêt général de l'Union susceptible de justifier des ingérences, même graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte »⁶⁹⁴. Dit autrement, les juges européens semblent envisager que la protection des droits et des libertés d'autrui découle aussi de la protection de la sécurité publique. C'est ainsi qu'un équilibre paraît être trouvé entre liberté individuelle et sécurité publique.

La multiplication des attentats terroristes sur le sol européen n'est pas sans incidence sur ce glissement quant à la manière de concevoir l'équilibre, même si les autres arrêts avaient été rendus durant une décennie caractérisée par le terrorisme qui a frappé la sécurité publique sur le sol européen. Ce changement a des répercussions notables sur la vie privée des citoyens européens. En validant en partie le système PNR, la Cour a reconnu que, bien que les données PNR puissent révéler des informations très détaillées sur la vie privée d'une personne, ces

⁶⁹¹ CJUE, 26 juillet 2017, avis 1/15, Point 148.

⁶⁹² S. PEYROU, « Accord PNR UE-Canada : validation par la CJUE du système PNR, des modalités à revoir ! », *GDR-ELSJ*, 28 juillet 2017, en ligne à URL : <http://www.gdr-elsj.eu/2017/07/28/informations-generales/accord-pnr-ue-canada-validation-cjue-systeme-pnr-modalites-a-revoir-reflexions-lavis-115-de-cjue-26-juillet-2017/> consulté le 21 août 2023.

⁶⁹³ CJUE, 21 décembre 2016, *Tele2 Sverige*, Point 103.

⁶⁹⁴ CJUE, 26 juillet 2017, avis 1/15, Point 149.

informations sont limitées à certains aspects spécifiques, notamment en ce qui concerne les voyages aériens entre le Canada et l'Union européenne⁶⁹⁵.

Les juges européens semblent admettre des restrictions importantes aux droits fondamentaux, au nom de la lutte contre le terrorisme, mettant en avant l'intérêt général associé à la sécurité publique. On peut penser que le traumatisme causé par le terrorisme est devenu si important qu'il permette une telle évolution dans la jurisprudence européenne qui va jusqu'à admettre des limitations dans les droits fondamentaux des citoyens européens, et pas n'importe lequel : le droit à la vie privée.

En effet, les juges européens ont adopté une approche plus souple dans cette affaire par rapport à leurs décisions antérieures. Contrairement à l'arrêt *Digital Rights Ireland*, où la Cour avait critiqué la surveillance généralisée appliquée même à des individus sans lien évident avec des infractions graves⁶⁹⁶, l'analyse actuelle considère que les données PNR seront traitées de manière systématique avant l'arrivée des vols au Canada. Ce traitement sera effectué par des moyens automatisés basés sur des critères préétablis, ce qui représente un changement notable dans l'appréciation de l'ingérence dans les droits fondamentaux⁶⁹⁷.

La Cour a adopté une nouvelle approche d'analyse en ne rejetant pas directement le mécanisme PNR, mais en procédant à un examen minutieux de son fonctionnement. Elle applique ses critères habituels pour évaluer la nécessité stricte de l'ingérence dans les droits fondamentaux, notamment le respect de la vie privée et la protection des données, tels qu'énoncés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, ainsi que le principe de proportionnalité⁶⁹⁸. C'est sur le fondement de la Charte qu'elle fonde la validation du système PNR.

Cependant, il convient de noter une incohérence dans le raisonnement des juges luxembourgeois. En relativisant la portée des droits fondamentaux énoncés dans la Charte, qu'ils considèrent non comme des prérogatives absolues mais comme devant être équilibrés par leur rôle dans la société, la Cour semble également s'appuyer sur le Préambule de la Charte, notamment son alinéa 4⁶⁹⁹. Ce dernier souligne la nécessité de renforcer la protection des droits fondamentaux en tenant compte de l'évolution sociale, du progrès et des avancées scientifiques et technologiques. Cette approche entraîne une relativisation des droits

⁶⁹⁵ Ibidem, point 150.

⁶⁹⁶ CJUE, *Digital Rights Ireland Ltd*, 8 avril 2014, Points 57 & 58.

⁶⁹⁷ CJUE, 26 juillet 2017, avis 1/15, point 131.

⁶⁹⁸ S. PEYROU, « Accord PNR UE-Canada : validation par la CJUE du système PNR, des modalités à revoir ! (Réflexions sur l'avis 1/15 de la CJUE, 26 juillet 2017) », *GDR-ELSJ*, 28 juillet 2017.

⁶⁹⁹ CJUE, 26 juillet 2017, avis 1/15, Point 136.

fondamentaux énoncés dans les articles 7 et 8 de la Charte, conduisant la Cour à modérer significativement sa jurisprudence antérieure⁷⁰⁰.

Il est toutefois crucial de souligner que la Cour n'examine qu'une seule des finalités de l'accord, bien qu'auparavant, elle ait également identifié deux autres aspects nécessitant la détermination d'une base légale appropriée⁷⁰¹. Deux raisons semblent pouvoir expliquer cette démarche. D'une part, l'objet du contrôle de la Cour ici est, semble-t-il, d'« examiner la compatibilité des mesures adoptées au titre de la sécurité et de la sûreté publique avec les exigences des articles 7 et 8 de la Charte »⁷⁰². Ainsi, les deux finalités du projet d'accord sont envisagées de façon hiérarchisée, eu égard aux exigences de la Charte des droits fondamentaux. D'autre part, l'examen limité à une seule finalité de l'accord pourrait refléter une forme d'autolimitation de la part de la Cour. En effet, il est possible que l'accord, tel qu'il est proposé, ne garantisse pas adéquatement la protection des données personnelles. Une telle analyse aurait pu entraîner des conséquences plus graves que celles issues des évaluations sur le critère de nécessité, car elle aurait pu mener à une annulation complète de l'accord, laissant peu de marge pour des ajustements lors des négociations ultérieures⁷⁰³.

Alors que l'arrêt *Tele2 Sverige* ouvrait la voie à une possible invalidation du système PNR dans son ensemble en raison de son traitement des passagers comme des suspects potentiels nécessitant surveillance, la Cour de Luxembourg a évité cette approche globale⁷⁰⁴. En effet, plutôt que de rejeter l'accord dans son intégralité, elle a choisi de mener une analyse approfondie des différentes mesures de l'accord pour évaluer spécifiquement leurs impacts sur les droits fondamentaux.

Sous-section 3 – Une limitation des droits fondamentaux au caractère disproportionné

La citoyenneté européenne octroie des droits et implique des devoirs, qui s'ajoutent à ceux qui sont attribués par la citoyenneté nationale. L'article 2 du TUE affirme ainsi que « L'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'Homme, y compris des droits des personnes appartenant à des minorités. Ces valeurs sont communes aux États membres dans une société caractérisée par le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité et

⁷⁰⁰ Ibidem

⁷⁰¹ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁷⁰² Ibidem.

⁷⁰³ Ibid.

⁷⁰⁴ M. BENLOLO-CARABO, « Protection des données personnelles, lutte contre le terrorisme : la CJUE confrontée à la surveillance de masse », *Chronique Droit pénal de l'Union européenne, Revue trimestrielle de droit européen*, n° 4, 2017, pp. 884-893.

l'égalité entre les femmes et les hommes »⁷⁰⁵. La mise en avant de la citoyenneté européenne participe au renforcement des droits des ressortissants des États membres.

À l'instar des citoyens nationaux, les citoyens de l'Union européenne ont des droits inhérents à leur qualité de citoyen européen⁷⁰⁶. Ces derniers sont garantis par les traités européens, dont le TFUE, qui, dans son article 16, affirme le droit à la protection des données à caractère personnel⁷⁰⁷. En effet, le traitement des données à caractère personnel est inscrit dans un cadre juridique européen qui cherche l'équilibre. Le droit à la protection des données à caractère personnel n'est pas considéré comme un droit absolu dès lors que le législateur considère, eu égard à sa fonction dans la société, que ce droit doit être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Ce dernier implique que seules les données à caractère personnel qui sont indispensables à l'opération envisagée peuvent faire l'objet d'un traitement.

Le droit européen cherche à concilier le principe de protection avec le droit à la liberté d'expression qui inclut le droit à la liberté de communication et d'information. Ce droit à la liberté d'expression est en effet un droit fondamental reconnu par plusieurs textes, dont l'article 10 de la Convention européenne des droits de l'Homme du 4 novembre 1950 et l'article 11 de la Déclaration des droits de l'Homme et du Citoyen du 26 août 1789. Le droit européen tente ainsi de créer, tant bien que mal, une balance des intérêts portés par plusieurs droits fondamentaux⁷⁰⁸.

La restriction des droits et libertés reconnus dans la Charte des droits fondamentaux de l'Union européenne est conditionnée au respect du principe de proportionnalité⁷⁰⁹. Les droits et libertés fondamentaux consacrés dans cette charte peuvent parfois entrer en contradiction. Cette situation invite les personnes concernées à recourir à une conciliation visant un juste

⁷⁰⁵ Article 2, Traité sur l'Union européenne, 2012.

⁷⁰⁶ C. RAPOPORT, « Nationalité et citoyenneté de l'Union européenne », in *La nationalité au carrefour des droits*, Presses universitaires de Rennes, 2019, pp. 89-103. Loge AD EUROPAM, « La citoyenneté européenne comme centre de l'union », *Humanisme*, 2017, pp. 47-53.

⁷⁰⁷ Vie publique, « Quels sont les droits et les devoirs du citoyen européen », *Fiche thématique*, 4 mars 2021.

⁷⁰⁸ E. BARBRY, « Le droit à la protection des données personnelles n'est pas un droit absolu face à la liberté d'information », *Le Monde du Droit*, 9 juillet 2021.

⁷⁰⁹ En France, cette limitation de la liberté d'expression a fait l'objet d'un sérieux débat, notamment dans une perspective comparatiste avec le droit américain. Voir en sens : I. BOUHADANA, W. GILLES, J. HARIVEL, "Freedom of expression and the values of the French Republic. Article dedicated to the memory of the victims of the terrorist attacks of 2015 in France", in Russell L. Weaver and Steven I. Friedland (Edited by), *Comparative Perspectives on Freedom of Expression, Global Papers Series*, Vol. II, Carolina Academic Press, 2017, pp. 141-158. Pour les auteurs de cet article, la liberté d'expression dans sa conception française se conçoit de manière négative, les citoyens sont libres de s'exprimer dès lors qu'ils ne causent pas de torts à autrui.

équilibre entre les deux principes en conflit. Ces exigences reposent alors sur le seul respect du principe de proportionnalité qui est un principe général du droit de l'Union européenne⁷¹⁰.

§ 1 – Une remise en cause de l'extension du domaine de la donnée

Prendre l'avion de nos jours implique d'entrer dans un domaine où la collecte de données personnelles est omniprésente. Le parcours de l'usager des aéroports est traversé non seulement par la collecte des données PNR et API, mais aussi des données à caractère personnel relatives aux passeports et cartes nationales d'identité qui comportent des informations biométriques, dont la reconnaissance faciale et les empreintes digitales⁷¹¹, le titulaire de ces derniers s'en dépossédant au bénéfice de l'État lors de leur constitution.

En France, le Conseil d'État a justifié cette ingérence en se basant sur l'argument que la collecte, la conservation et le traitement des informations personnelles nominatives par une autorité publique sont nécessaires pour exercer le droit au respect de la vie privée, dans un contexte de sécurité publique⁷¹². La délimitation des droits fondamentaux au nom de la sécurité collective ou de l'intérêt général est évidente dans nos aéroports aujourd'hui. En Europe, les attaques terroristes ont touché plusieurs États européens, telle l'attaque contre l'aéroport de Bruxelles en mars 2016⁷¹³. Ces événements tragiques ont renforcé l'idée selon laquelle l'ingérence dans les droits fondamentaux des citoyens européens est nécessaire pour sauvegarder la sécurité de ces derniers face aux infractions terroristes.

Cette utilisation accrue des données personnelles, au nom de la sécurité publique et au détriment des droits fondamentaux, se fait dans un contexte de développement du domaine de la donnée-sans forcément qu'il existe un élargissement consécutif de la protection des données à caractère personnel⁷¹⁴. En ce sens, Valérie-Laure Benabou a pu faire le constat en 2018 d'une « dangerosité accrue des moyens informatiques pour les libertés du citoyen. La Deuxième guerre mondiale était toujours présente dans les esprits et, avec elle, la dérive du fichage des individus ayant conduit à des déportations ou autres sinistres finalités »⁷¹⁵. Depuis lors, le développement de l'informatique et l'accroissement exponentiel des capacités de traitement de la donnée n'a fait que confirmer ces inquiétudes.

⁷¹⁰ Jean-Marc Sauvé estime que le principe de proportionnalité s'est affirmé depuis plus d'un siècle en France comme un outil de protection efficace des libertés et des droits fondamentaux mais il subit depuis quelques années une influence européenne qui le transforme de manière concrète. J-M. SAUVÉ, « Le principe de proportionnalité, protecteur des libertés ? », *Les cahiers Portalis*, 2018, pp. 9-21.

⁷¹¹ « L'identification biométrique et la sécurité publique », *Dalloz IP/IT*, mars 2019.

⁷¹² Conseil d'État, ass., 26 oct. 2011, n° 317827.

⁷¹³ « Zaventem, un aéroport cible en 1979 d'une attaque terroriste », *Ouest-France*, 22 mars 2016.

⁷¹⁴ V-L. BENABOU, « L'extension du domaine de la donnée », *Légipresse*, n° 359, avril 2018, p.197.

⁷¹⁵ Ibidem. Voir aussi R. POZNANSKI, « Le fichage des juifs de France pendant la Seconde Guerre mondiale et l'affaire du fichier des juifs », *Gazette des archives*, 1997, pp. 250-270.

Nourrie par le Big Data⁷¹⁶, la « datafication » progressive de la vie des femmes et des hommes de notre époque n'oublie pas les passagers aériens⁷¹⁷. Or, cette extension du domaine de la donnée a pour conséquence d'élargir le champ des menaces qui pèsent sur les passagers aériens. Elle rend ainsi indispensable l'intervention des institutions pour sauvegarder les droits fondamentaux du citoyen dont le droit à la protection de la vie privée et le droit à la protection des données personnelles.

Telle est la démarche retenue par l'arrêt Digital Rights Ireland⁷¹⁸ qui a invalidé la directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou des réseaux publics de communications. En effet, la Cour a considéré en l'espèce que les règles européennes constituaient une ingérence particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel affirmés par la Charte des droits fondamentaux de l'Union européenne dans leurs articles 7 et 8⁷¹⁹.

Les juges de Luxembourg ont reconnu que l'ingérence était justifiée par des objectifs d'intérêt général, comme la lutte contre le terrorisme et la criminalité organisée. Cependant, ils l'ont jugée disproportionnée, car elle s'appliquait de manière généralisée à toutes les personnes, à tous les moyens de communication électronique et à l'ensemble des données de trafic, sans distinction ni limitation en fonction des objectifs poursuivis. De plus, l'absence de critères objectifs pour restreindre l'accès et l'utilisation des données par les autorités, ainsi que l'absence de mention claire de la durée de conservation, a été critiquée.⁷²⁰

Il est à cet égard utile de rappeler que l'article 52 de la Charte des droits fondamentaux prévoit que « toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus

⁷¹⁶ V. MAYER-SCHÖNBERGER, « La révolution Big Data », *Politique étrangère*, 2014, pp. 69-81. L'auteur insiste sur le caractère politique de cet instrument économique qui a un impact considérable sur notre manière de voir et de comprendre le monde. Ce terme de Big Data fait référence à des ensemble de données trop volumineux et complexes pour les applications traditionnelles de traitement et collecte des données (voir la définition de la CNIL en ce sens <https://www.cnil.fr/fr/definition/big-data#:~:text=On%20parle%20depuis%20quelques%20ann%C3%A9es,%2C%20photos%2C%20vid%C3%A9os%2C%20etc>).

⁷¹⁷ V.-L. BENABOU, « L'extension du domaine de la donnée », *Légipresse*, n° 359, avril 2018, p.197.

⁷¹⁸ CJUE, Rights Ireland Affaire C-293/12 (Affaires jointes C-293/12, C-594/12).

⁷¹⁹ Charte des droits fondamentaux de l'Union européenne.

⁷²⁰ V.-L. BENABOU, op. cit.

par l'Union ou au besoin de protection des droits et libertés d'autrui »⁷²¹. Cette règle de l'Union européenne fait écho aux dispositions de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales⁷²² qui admettent des limites aux principes de protection des droits fondamentaux⁷²³.

Or, cela n'a pas forcément été interprété par la CJUE comme la reconnaissance d'une large marge d'appréciation confiée aux institutions de l'Union européenne. Par conséquent, la condition de nécessité de l'article 52 de la Charte est interprétée au sens de « strict nécessaire » par les juges européens⁷²⁴ qui ont été amenés à examiner la proportionnalité des mesures annoncées de façon rigoureuse. Dans son avis sur l'accord PNR EU-Canada, les juges de Luxembourg ont reproché à l'accord des dispositions imprécises, créant un danger pour les droits fondamentaux, et proposé des améliorations en matière de traitement, conservation et utilisation des données.

§ 2 – Une critique du manque de précision des dispositions de l'accord

Dans son avis au point 181, la Cour a jugé que les conditions énoncées dans l'article 3, paragraphe 5, sous a) et b), de l'accord proposé, permettant au Canada de traiter les données PNR, manquaient de clarté et de précision. Elle a estimé que ces dispositions étaient formulées de manière trop vague et générale, et ne répondaient donc pas aux exigences de limitation strictement nécessaire pour atteindre les objectifs de l'accord⁷²⁵. Cette analyse approfondie de l'accord a ainsi conduit la Cour à considérer les dispositions incompatibles avec le droit européen, telles que l'article 3 du projet d'accord qui autorise l'autorité canadienne compétente à traiter les données PNR lorsqu'il est nécessaire.

Il en va de même pour les 19 catégories de données PNR énumérées dans l'annexe de l'accord proposé, qui, selon la Commission, correspondent à l'annexe I des lignes directrices de l'Organisation de l'aviation civile internationale (OACI) sur les données PNR. Cependant, comme l'a souligné l'avocat général dans ses conclusions, certaines rubriques, notamment celle concernant les informations sur les grands voyageurs et les programmes de fidélisation, ainsi que celle couvrant toutes les coordonnées disponibles, ne définissent pas de manière

⁷²¹ Article 52, Charte des droits fondamentaux.

⁷²² Convention de sauvegarde des droits de l'Homme et des libertés fondamentales.

⁷²³ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁷²⁴ CJCE, 15 décembre 2008, Aff. C-73/07, Satakunnan Markkinapörssi et Sanoma Media : Rec. 2008, I, P. 9831, pt 56.

⁷²⁵ CJUE, 26 juillet 2017, avis 1/15, Point 181.

suffisamment claire et précise les données PNR à transférer⁷²⁶. La Cour identifie ici le caractère insuffisamment précis de l'accord envisagé à l'égard des données PNR à transmettre puisque la rubrique 5, par exemple, avec l'emploi du terme « etc. » ne caractérise pas suffisamment l'étendue des données à transférer⁷²⁷.

D'autres rubriques ont été critiquées pour leur imprécision, c'est le cas de la rubrique 17 qui vise « les remarques générales, y compris les données OSI (Other Supplementary Information) les données SSI (Special Service Information) et les données SSR (Special Service Request) ». Les juges ont considéré que cette rubrique de « texte libre » ne fournit « aucune indication sur la nature et l'étendue des renseignements qui doivent être transmis, et paraît même susceptible d'englober des informations dépourvues de tout rapport avec la finalité du transfert des données PNR »⁷²⁸. Ce type de « free text » fragilise la protection des données personnelles et de la vie privée du passager puisque les opérateurs aériens pourraient y insérer tout type d'informations, ce qui conduirait à un élargissement du champ matériel des données transférées.

Il n'est pas exclu que ces informations puissent révéler des données sensibles, tels que l'état de santé, l'origine ethnique ou les convictions religieuses de la personne concernée ou de ses compagnons de voyage⁷²⁹. La présence de ces données sensibles pose un problème au regard de l'article 21 de la Charte des droits fondamentaux, qui interdit toute discrimination fondée sur des critères tels que le sexe, la race, l'origine ethnique, la religion, ou les convictions personnelles⁷³⁰.

Les données collectées par les transporteurs sont susceptibles d'être utilisées à des fins de profilage dans le but de lutter contre les infractions terroristes et de crimes organisés. Or, l'utilisation des données sensibles, collectées par cette rubrique « texte libre », dans le cadre de la lutte contre le terrorisme et la criminalité transnationale, constitue une violation de la Charte des droits fondamentaux. Cette prise de position des juges de Luxembourg nous paraît subtile dans le contexte de menaces terroristes de ces dernières décennies.

Cet avis montre la détermination de la Cour à protéger les libertés individuelles, même dans un contexte de sécurité publique. La Cour réaffirme que les données sensibles ne doivent pas être transférées vers un État tiers, sauf si une justification précise et particulièrement solide,

⁷²⁶ Ibidem, point 156.

⁷²⁷ Ibid.

⁷²⁸ Ibidem, point 160.

⁷²⁹ Conclusions de l'avocat général dans la demande d'avis 1/15, Luxembourg, le 8 septembre 2016, Point 212.

⁷³⁰ Article 21, Charte des droits fondamentaux de l'Union européenne.

fondée sur des motifs autres que la simple protection contre le terrorisme et la criminalité transnationale, est présentée⁷³¹.

§ 2 – Un insatisfaisant traitement automatisé des données PNR

Les juges de Luxembourg ont mené une analyse minutieuse du traitement automatisé des données personnelles des passagers aériens dans le cadre de l'accord PNR UE-Canada. D'abord, la Cour est revenue sur les conclusions de l'avocat général qui avait considéré que ces données allaient être « soumises à des analyses par des moyens automatisés, fondés sur des modèles et des critères préétablis et sur des recoupements avec diverses bases de données »⁷³². La Cour n'a en effet pas été convaincue par la justesse de cette analyse puisqu'elle a considéré qu'à partir du moment où ces analyses sont « effectuées à partir de données à caractère personnel non vérifiées et où elles se fondent sur des modèles et des critères préétablis »⁷³³, le traitement présentera fort probablement un taux d'erreur important, conformément à ce qu'avaient affirmé le Gouvernement français et la Commission européenne⁷³⁴. La Cour a rappelé que le CEPD avait confirmé ce risque de taux d'erreur dans leur avis sur le projet de proposition de décision-cadre du Conseil⁷³⁵.

Elle indiqua également que l'accord en question doit veiller à ce que les bases de données avec lesquelles les données personnelles PNR sont recoupées « doivent être fiables, actuelles et limitées à des bases de données exploitées par le Canada en rapport avec la lutte contre le terrorisme et la criminalité transnationale grave »⁷³⁶. Alors que l'avocat général ne proposait que des garde-fous, les juges de Luxembourg ont précisé que les critères d'évaluation ne pourraient se fonder sur l'origine ethnique d'une personne, sa religion ou ses convictions philosophiques, ses opinions politiques, son appartenance syndicale, son état de santé ou son orientation sexuelle. La Cour a ainsi fourni des indications concrètes sur les critères à appliquer pour les autorités canadiennes alors que l'avocat général « préconisait de chercher à éviter une utilisation potentiellement discriminatoire des données PNR »⁷³⁷.

La conservation et l'utilisation des données personnelles des passagers aériens a également été pointée du doigt par les juges de Luxembourg. En effet, la Cour a indiqué que « dès lors

⁷³¹ CJUE, 26 juillet 2017, avis 1/15, Point 161.

⁷³² Conclusions de l'avocat général dans la demande d'avis 1/15, Luxembourg, le 8 septembre 2016, Point 130 à 132.

⁷³³ CJUE, 26 juillet 2017, avis 1/15, Point 169.

⁷³⁴ Ibidem

⁷³⁵ Projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record – PNR) à des fins répressives, JO 2008, C 110, p. 1.

⁷³⁶ CJUE, 26 juillet 2017, avis 1/15, Point 172.

⁷³⁷ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

que les passagers aériens ont, après vérification de leurs données PNR, été admis à entrer sur le territoire de ce pays tiers, une utilisation desdites données pendant leur séjour au Canada doit se fonder sur des circonstances nouvelles justifiant cette utilisation », sous le contrôle d'une autorité administrative indépendante ou un juge intervenant à la suite d'une demande motivée des autorités compétentes⁷³⁸. Le juge européen appliqua ce faisant au projet d'accord PNR EU-Canada sa jurisprudence *Tele2 Sverige*, soulignant ainsi qu'à ses yeux « la question du contrôle préalable effectué par une juridiction est elle aussi centrale »⁷³⁹. Comme ils l'avaient conclu dans l'affaire *Tele2 Sverige*, les juges de Luxembourg ont considéré que l'utilisation des données personnelles des passagers aériens « doit faire l'objet d'une information de la personne concernée, sauf lorsque cela est susceptible de compromettre les enquêtes conduites par les autorités publiques »⁷⁴⁰ afin de permettre aux passagers d'appliquer leur droit d'accès et de rectification des informations, voire d'exercer de manière effective un recours juridictionnel.

La Cour de justice a, par ailleurs, validé le principe d'une durée de cinq ans pour le stockage des données des passagers aériens⁷⁴¹. En revanche, elle s'est opposée au stockage continu des données de l'ensemble des passagers voyageant au Canada. En effet, selon la Cour, les États ne doivent conserver que les données des passagers représentant un danger en termes de terrorisme ou de criminalité organisée transnationale⁷⁴², reprenant ici la solution de l'arrêt *Tele2 Sverige* qui prône la conservation ciblée des données⁷⁴³. Cette dernière exigence est critiquable pour certains commentateurs⁷⁴⁴, car l'interdiction de stockage continu nuirait à la sécurité et la sûreté publiques dans la mesure où la destruction « des données de la majorité des passagers à l'occasion de leur départ du Canada » permet aux passagers suspects qui effectuent des trajets de manière régulière d'éviter d'être identifiés par les autorités aéroportuaire compétentes. Cela nuirait donc, selon ces mêmes commentateurs, à l'accomplissement de l'un des objectifs essentiels de l'accord : prévenir les suspects d'utiliser les transports aériens pour la commission d'infractions terroristes ou de crimes transnationaux organisés.

⁷³⁸ CJUE, 26 juillet 2017, avis 1/15, Point 200.

⁷³⁹ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

⁷⁴⁰ *Ibidem*

⁷⁴¹ CJUE, 26 juillet 2017, avis 1/15, Point 209.

⁷⁴² *Ibidem*, point 207.

⁷⁴³ CJUE, 21 décembre 2016, *Tele2 Sverige*, Point 108.

⁷⁴⁴ V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *LexisNexis*, 6 juin 2018.

Chapitre 2 – Les institutions européennes, une protection juridique déséquilibrée des dossiers passagers

« Rien n'est possible sans les hommes, rien n'est durable sans les institutions (...). Les institutions peuvent, si elles sont bien construites, accumuler et transmettre la sagesse des générations successives » écrivait Jean Monnet dans ses Mémoires en 1976⁷⁴⁵. Ainsi, pour assurer l'efficacité de la construction européenne, les États membres ont opté pour un système composé de plusieurs institutions se partageant les pouvoirs exécutif, législatif et judiciaire. L'Union européenne, telle que nous la connaissons aujourd'hui, est le résultat d'un ensemble d'avancées en matière de construction européenne dont l'origine peut être trouvée dans la Déclaration Schuman de mai 1950. Ce projet d'expansion au-delà des frontières nationales s'est d'abord matérialisé par la mise en place de la Communauté européenne du charbon et de l'acier (CECA) en 1951, puis de la Communauté économique européenne (CEE) en même temps que la Communauté européenne de l'énergie atomique (CEEa) en 1957. L'Union européenne actuelle date du 1^{er} novembre 1993, date de la prise d'effet du Traité de Maastricht signé par les États membres, au nombre de douze à l'époque, le 7 février 1992⁷⁴⁶, après d'âpres négociations. L'Union européenne est fondée sur trois piliers, à savoir la Communauté européenne (qui a remplacé la CEE, la CECA et la CEEa), la Politique étrangère et de sécurité commune (PESC) et la Justice et affaires intérieures (JAI). Avant même la création de l'Union, la construction européenne s'était déjà approfondie avec l'adoption d'un traité, l'Acte unique européen entré en vigueur en 1987, qui constituera une étape importante du projet européen avec la création d'un cadre juridique qui permettra plus tard à l'Union européenne de signer des traités internationaux et de lui confier un rôle sur la scène internationale⁷⁴⁷.

Le Traité de Lisbonne, signé le 13 décembre 2007 et entré en vigueur en 2009, encadre désormais le fonctionnement de l'Union européenne après le rejet d'un traité établissant une constitution pour l'Europe (TECE). Il a adapté en profondeur les règles des anciens traités pour permettre une meilleure coordination des 27 États membres. La Communauté

⁷⁴⁵ J. MONNET, *Mémoires*, Fayard, 1976. Pour le père fondateur du projet européen, celui-ci devait : « Unir les hommes, régler les problèmes qui les divisent, les amener à voir leur intérêt commun », pour lui, la direction est d'aller vers « tout ce qui ira dans le sens d'une communauté plus large des peuples et de la transformation de la forme capitaliste du passé vers une meilleure répartition entre les citoyens du produit de leur effort commun ».

⁷⁴⁶ J.-C. ZARKA, *L'essentiel des institutions de l'Union européenne*, Lextenso, 2020.

⁷⁴⁷ Ibidem

européenne disparut et l'Union a été dotée de la personnalité juridique⁷⁴⁸. C'est dans ce cadre d'intégration renforcée qu'en mai 2016, l'Union européenne a adopté un train de mesures afin de mieux protéger les données à caractère personnel en vue d'adapter l'Europe à l'ère numérique. Plus de 90% des Européens peuvent ainsi revendiquer les mêmes droits en matière de données personnelles dans toute l'Union européenne, où que soient traitées ces données⁷⁴⁹.

Le 26 janvier 2022, la Commission a proposé une déclaration européenne sur les droits et principes numériques pour la décennie numérique. Ce projet est intervenu dans le prolongement de sa communication intitulée « Boussole numérique 2030 : une vision européenne pour la décennie numérique ». Ce document expose la vision d'un espace transformé sur le plan numérique d'ici 2030, conformément aux valeurs prônées par les Européens. En effet, l'ambition de l'Union européenne semble d'atteindre une certaine souveraineté sur le plan numérique dans un monde interconnecté et ouvert mais non sans compétition entre différents systèmes de valeurs. Cette vision européenne se base sur l'idée de citoyens autonomes et d'entreprises innovantes dans « une société numérique centrée sur l'humain, inclusive, prospère et durable »⁷⁵⁰.

Dans cette déclaration commune, les trois institutions européennes, le Parlement, le Conseil et la Commission, se sont mises d'accord sur des engagements politiques et des droits communs dans un environnement marqué par la transformation numérique, où l'intégration de la technologie digitale concerne l'ensemble des activités des individus et des entreprises. Cette initiative politique européenne encourage les principes suivants : la sauvegarde des droits fondamentaux en ligne ; l'utilisation de la technologie pour rassembler les gens ; la garantie de l'accès aux services publics en ligne ; le droit à la déconnexion ; la liberté de choisir d'utiliser et d'interagir avec les systèmes d'intelligence artificielle ; la vie privée ; le contrôle des données à caractère personnel ; l'accès à des technologies sûres ; la promotion de technologies numériques durables⁷⁵¹.

⁷⁴⁸ Ibid.

⁷⁴⁹ Union européenne, « Protection des données personnelles », *Commission Européenne*, 2024, disponible à URL : https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_fr consulté en ligne le 5 mai 2024.

⁷⁵⁰ Communiqué de presse, « Les institutions européennes approuvent la déclaration sur les droits et principes numériques », *Parlement européen*, 15 décembre 2022.

⁷⁵¹ Ibidem

Avec la signature du Traité de Lisbonne⁷⁵², la protection des données à caractère personnel est devenue un droit fondamental reconnu par le Traité sur le fonctionnement de l'Union européenne et la Charte des droits fondamentaux de l'Union européenne (dont l'article 8 de la reconnaît pour toute personne résidant dans l'UE le droit à la protection des données à caractère personnel la concernant, le droit d'accéder aux données collectées la concernant et d'en obtenir rectification)⁷⁵³. Ainsi, les Européens disposent dorénavant d'une base juridique spécifique qui leur permet d'adopter des textes législatifs pour protéger ce droit fondamental.

Les institutions européennes⁷⁵⁴ partagent toutefois des positions différentes quant à la protection des données personnelles des passagers aériens. On note une tension entre, d'un côté, la nécessité de renforcer la sécurité publique et, d'un autre, la nécessité de préserver les libertés fondamentales. Face à la réalité des rapports de force au sein des relations internationales, le Conseil de l'Union européenne et la Commission européenne ont été peu enclins à mettre en avant la protection de la vie privée et des données personnelles pour privilégier la sécurité publique (section 1). Ce renoncement à défendre vigoureusement les droits fondamentaux des passagers aériens a été contrebalancé par la Cour de justice de l'Union européenne, le Parlement et le Comité européen de la protection des données qui sont devenus les garants de ces droits (section 2).

Section 1 – Des acteurs initiateurs d'un cadre juridique favorable à la sécurité publique : le Conseil de l'Union européenne et la Commission

Les développements technologiques rapides et étendus des deux dernières décennies ont créé de nouveaux défis en matière de protection des données personnelles. Le partage et la collecte de données a augmenté de façon exponentielle, la plupart du temps à l'échelle mondiale, les individus publiant de plus en plus de données à caractère personnel accessibles à tous⁷⁵⁵. L'intégration économique et sociale résultant du fonctionnement du marché intérieur a également donné lieu à une augmentation considérable des flux transfrontaliers de données⁷⁵⁶.

Afin de tenir pleinement compte de toutes ces évolutions et de promouvoir l'économie numérique, les institutions européennes sont conscientes qu'il est nécessaire d'assurer un

⁷⁵² Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne le 13 décembre 2007. Adopté en 2007, le Traité de Lisbonne vise l'encadrement du fonctionnement de l'Union européenne. Il est entré en vigueur le 1^{er} décembre 2009.

⁷⁵³ P. GILLIAUX, « Le Traité de Lisbonne », *Courrier hebdomadaire du CRISP*, pp. 5-83.

⁷⁵⁴ J-L. QUERMONNE, « Les institutions de l'Union européenne après le Traité de Lisbonne », *L'Europe en formation*, 2011, pp. 31-44.

⁷⁵⁵ M. GALLET, « La France et l'Europe face à l'enjeu du Big Data, l'exemple de la collecte et du traitement des données médiatiques », *Géoéconomie*, 2014, pp. 7-23.

⁷⁵⁶ L. AZOULAI, « Le marché intérieur », *Politiques européennes*, Presses de Science Po, 2009.

niveau élevé de protection des données à caractère personnel tout en permettant la libre circulation de ces données⁷⁵⁷.

En ce qui concerne les données à caractère personnel utilisées à des fins répressives, les autorités des États membres ont un besoin accru de les traiter et les échanger dans le cadre de la lutte contre la criminalité transnationale et le terrorisme. Dans ce contexte, la mise en place de règles claires et cohérentes en matière de protection des données au niveau de l'Union européenne est devenue indispensable pour améliorer la coopération entre ces autorités.

Principal organe de décision de l'UE avec le Parlement, le Conseil a mis en avant le PNR comme un outil de sécurité collective (sous-section 1) en mandant la Commission pour négocier avec ses homologues américains le projet PNR, sans prendre en compte les réticences des autres institutions vis-à-vis de ce dernier (sous-section 2).

Sous-section 1 – Le Conseil de l'Union européenne, promoteur de la sécurité collective

Reconnu comme étant la voix des États membres de l'Union européenne, le Conseil adopte la législation et coordonne les politiques de l'UE dont la promotion de la sécurité collective. Il conclut ainsi les accords PNR signés entre l'UE et des pays tiers. Il a également été l'architecte, aux côtés du Parlement européen, de la directive européenne PNR.

§ 1 – Le Conseil de l'Union européenne, la voix des États membres

Le Conseil de l'Union européenne (ci-après « le Conseil ») est constitué des ministres des États membres, compétents dans des domaines spécifiques tels que les affaires étrangères, l'économie, les affaires sociales, la justice et les affaires intérieures. En vertu de l'article 16 du Traité sur l'Union européenne (TUE), le Conseil exerce, conjointement avec le Parlement européen, les pouvoirs législatif et budgétaire⁷⁵⁸.

Dans le schéma institutionnel européen, le Conseil constitue, avec le Parlement européen, le principal organe de décision de l'UE. Historiquement⁷⁵⁹, il a succédé au Conseil des ministres après l'entrée en vigueur du Traité de Maastricht⁷⁶⁰. Avec la réforme institutionnelle

⁷⁵⁷ C. GAGLIO, S. GUILLOU, « L'Europe numérique, entre singularités, faiblesses et promesses », *Revue de l'OFCE*, 2018, pp. 11-36. Pour les auteurs de cet article, l'Europe peine à avoir une politique numérique qui ferait d'elle une puissance dans ce domaine malgré des dépenses en recherche et développement de 300 milliards d'euros, ses 512 millions d'habitants et son statut de deuxième zone géographique la plus prospère dans le monde.

⁷⁵⁸ TUE, article 16, alinéa 1. Voir. C. MESTRE, « Conseil de l'Union européenne », *Répertoire de droit européen*, Dalloz, octobre 2021.

⁷⁵⁹ Union européenne, décision n° 93/591 du Conseil, 8 novembre 1993, JOCE, n° L. 281, 16 novembre 1993.

⁷⁶⁰ Traité sur l'Union européenne tel que modifié par le Traité d'Amsterdam du 2 octobre 1997. Voir E. KESSOUS, « Le Traité de Maastricht : un coup d'État monétaire », *Vacarme*, 1997, p. 33. Voir aussi B. NIVET,

introduite par le Traité de Lisbonne, applicable depuis le 1^{er} décembre 2009, le partage des pouvoirs avec le Parlement européen est devenu l'une des caractéristiques du système décisionnel européen. Toutefois, le Conseil garde le monopole sur certaines questions, notamment en matière de coopérations renforcées ou de politique étrangère et de sécurité commune⁷⁶¹.

Revêtant une structure intergouvernementale, le Conseil représente chaque État membre au niveau ministériel, d'après l'article 16 TUE⁷⁶². L'État membre peut dès lors exprimer sa position, et par là même défendre ses intérêts lorsqu'un futur acte de l'Union est discuté, ou dès lors qu'un vote a lieu. Le déroulement de l'examen et l'adoption des actes de l'UE obéissent aux dispositions des traités européens et du règlement intérieur du Conseil.

Les ministres de l'Union européenne se réunissent en public lorsqu'ils délibèrent ou votent des projets d'actes législatifs. Les décisions sont, en principe, prises à la majorité qualifiée, soit 55 % des pays, 15 pays sur 27, représentant au moins 65 % de la population totale de l'Union⁷⁶³. Cependant, quatre pays, représentant au moins 35% de la population totale de l'UE, peuvent bloquer une décision. Par ailleurs, une exception existe pour les sujets sensibles, tels que la politique étrangère ou la fiscalité, qui nécessitent un vote à l'unanimité, autrement dit, un vote favorable de tous les pays. Aussi, la majorité simple est requise pour les questions procédurales et administratives.

Loin de ressembler à une conférence diplomatique, le Conseil est bien une institution communautaire, comme le rappelle l'article 13 TUE⁷⁶⁴, bien que les représentants des gouvernements des États membres « peuvent utiliser les sessions du Conseil pour aborder toute question qu'ils peuvent juger utile et *in fine* adopter des décisions, celles-ci n'étant pas alors des décisions de l'Union mais des décisions des représentants des États membres réunis en Conseil »⁷⁶⁵. L'action du Conseil n'est pas sans contrepoids. En effet, la Cour de justice opère un contrôle matériel et peut requalifier une décision, comme elle l'a affirmé dans son arrêt Parlement c/ Conseil et Commission, le 30 juin 1993⁷⁶⁶.

« De Maastricht à Nice : la laborieuse ascension de l'Union européenne », *Revue internationale et stratégique*, 2001, pp. 135-142.

⁷⁶¹ C. MESTRE, « Conseil de l'Union européenne », *Répertoire de droit européen*, Dalloz, octobre 2021.

⁷⁶² TUE, article 16, alinéa 2.

⁷⁶³ TUE, article 16, alinéa 3. Lire en ce sens. Union européenne, « Comment fonctionne le Conseil ? », Conseil de l'Union européenne, 2022, disponible à URL : https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/council-european-union_fr consulté en ligne le 29 mars 2023.

⁷⁶⁴ TUE, article 13.

⁷⁶⁵ C. MESTRE, « Conseil de l'Union européenne », *Répertoire de droit européen*, Dalloz, octobre 2021.

⁷⁶⁶ CJCE, 30 juin 1993, Parlement c/ Conseil et Commission, aff. C-181/91 et C-6248/91, Rec. I. 3685.

En outre, en plus de sa consécration comme institution, le Conseil est devenu avec le Traité de Lisbonne l'instance majeure de l'Union européenne, bien que ses attributions n'aient pas été substantiellement modifiées. Par ailleurs, son président est désormais « le visage et la voix de cette Union »⁷⁶⁷. Dans ce contexte décisionnel et structurel, cette institution se trouve quelque peu limitée dans ses prérogatives, prise entre un Conseil européen en pleine transformation et un Parlement renforcé, dont la majorité des revendications ont finalement été acceptées⁷⁶⁸.

Le Traité de Lisbonne a introduit une rupture considérable en instaurant la règle « un État, une voix », au détriment d'un système de pondération. Ce changement témoigne de la mutation de l'Union européenne⁷⁶⁹ d'une entité à vocation économique et commerciale à une entité politique. De fait, le Traité maintient la majorité qualifiée mais étend considérablement son champ d'application. Ce faisant, il initie un abandon progressif du droit de veto⁷⁷⁰. Par ailleurs, une présidence collective de trois États membres sur une période de dix-huit mois se superpose à la présidence tournante de six mois⁷⁷¹.

Enfin, une exception a été introduite dans l'organisation de cette présidence tournante avec la création du poste de haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, qui préside la formation du Conseil « Affaires étrangères »⁷⁷². Les autres réunions du Conseil sont présidées par le ministre compétent du pays assurant la présidence tournante de l'Union.

§ 2 – Le Conseil de l'Union européenne, organe décisif dans l'adoption des règles PNR

Dans le cadre des règles régissant le PNR, le Conseil a participé, d'une part, à l'adoption des actes législatifs qui ont mis en place le cadre juridique européen encadrant l'utilisation des dossiers passagers et, d'autre part, à la conclusion des accords internationaux PNR avec les autres États.

Comme rappelé précédemment (sous-section 2, section 2, chapitre 1), le Conseil de l'Union européenne n'a pas mis en avant, de manière effective, la protection des droits fondamentaux lors des négociations de l'accord PNR avec les États-Unis⁷⁷³, comme l'attendaient le

⁷⁶⁷ C. MESTRE, op. cit.

⁷⁶⁸ Ibidem

⁷⁶⁹ G. BOISMENU, I. PETIT, *L'Europe qui se fait : Regards croisés sur un parcours inachevé*, Presses de l'Université de Montréal, 2008, en ligne à URL : <http://books.openedition.org/pum/15196> consulté le 2 novembre 2023.

⁷⁷⁰ C. MESTRE, « Conseil de l'Union européenne », *Répertoire de droit européen*, Dalloz, octobre 2021.

⁷⁷¹ Ibidem

⁷⁷² Ibid.

⁷⁷³ Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure, 2012.

Parlement et le Comité européen de la protection des données. Dans ces négociations, le Conseil a donné mandat à la Commission pour négocier, au nom de l'UE, cet accord entre l'Union et les États-Unis. À la fin des négociations, sur la base d'une proposition de la Commission, le Conseil s'est prononcé sur la signature et la conclusion de l'accord PNR. Il a ensuite adopté la décision finale relative à sa conclusion.

Nonobstant des avis critiques envers l'accord PNR conclu avec les États-Unis, le Parlement, à travers la résolution du 5 mai 2010, a décidé de reporter le vote sur la demande d'approbation de cet accord. Ce dernier faisait valoir que certaines conditions minimales devaient être remplies afin de satisfaire aux exigences européennes de protection des droits fondamentaux. Il a ainsi fait usage de sa nouvelle prérogative, issue du Traité de Lisbonne, consistant à user d'un pouvoir d'approbation sur les accords négociés entre l'Union européenne et les États tiers, en vue de leur conclusion⁷⁷⁴.

Le 2 décembre 2010, le Conseil a autorisé la Commission à négocier un accord sur le transfert des données PNR avec les États-Unis. Un nouvel accord PNR a été paraphé le 17 novembre 2011⁷⁷⁵. Le Conseil a ici joué un rôle de colégislateur dont l'objectif était d'éviter un vide juridique, au prix d'un accord qui s'éloigne des standards habituels de protection des droits fondamentaux défendus par le droit européen en matière, notamment, de vie privée et de données personnelles. Cet accord déséquilibré⁷⁷⁶ s'est conclu dans un contexte international où la sécurité des États a été mise à mal. Le Conseil a probablement pensé « qu'il était préférable de conclure rapidement un accord sans se montrer trop pointilleux, dans un premier temps, sur des exigences visiblement incompréhensibles outre-Atlantique au regard de l'enjeu, dans l'espoir d'une solution plus globale, multilatérale et équilibrée à terme »⁷⁷⁷. C'est pourquoi le Conseil a mis en avant deux motifs qui, selon lui, justifiaient la conclusion de cet accord : « la situation d'incertitude dans laquelle se trouvent les compagnies aériennes et les passagers » et la nécessité « de protéger les intérêts financiers des parties concernées ». Effectivement, la violation de la législation américaine exposait les compagnies à des amendes de l'ordre de 5 000 \$ et à la privation du droit d'atterrissage⁷⁷⁸.

⁷⁷⁴ S. PEYROU, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », Droits fondamentaux, Europe, *Revue Mensuelle LexisNexis Jurisclasseur*, juillet 2012.

⁷⁷⁵ COM(2011) 807 final, 23 nov. 2011.

⁷⁷⁶ F. MARIATTE, « Protection des données personnelles des usagers des transports aériens », *Nouvelles technologies*, Dalloz, Europe n° 7, comm. 256, juillet 2004,

⁷⁷⁷ Ibidem

⁷⁷⁸ C. CHIAMBARETTO, E. COMBE, « L'écosystème du transport aérien et sa régulation », in *Le transport aérien*, La Découverte, 2023, pp. 29-56.

Puis, des négociations ont été ouvertes en vue de la conclusion d'un accord PNR entre l'Union européenne et le Canada. Les deux parties ont finalement signé, le 25 juin 2014, un accord sur le traitement de données des dossiers passagers et le transfert de ces données par les transporteurs aériens aux autorités canadiennes compétentes. Ce dernier remplaça l'accord en vigueur depuis 2006. Le Parlement européen a ensuite été invité à approuver l'accord. Cette approbation est une condition préalable à l'adoption, par le Conseil, d'une décision sur la conclusion de l'accord.

Dans le cadre des accords PNR avec le Canada⁷⁷⁹, la Commission a présenté en septembre 2010 une communication relative à la démarche globale adoptée en matière de transfert des données PNR aux pays tiers. Par la suite, en réponse à une demande du Conseil, la Commission a présenté en janvier 2011 une proposition visant à établir un système de données PNR à l'échelle de l'UE pour la protection contre les infractions terroristes et les formes graves de criminalité. Le Conseil a adopté son orientation générale dès le mois d'avril 2012. L'accord issu des négociations avec le Canada a été paraphé en 2013, puis le Conseil a adopté une décision⁷⁸⁰ relative à la conclusion de l'accord⁷⁸¹. En novembre 2014, le Parlement a saisi la Cour de justice de l'Union européenne afin que cette dernière détermine si l'accord était conforme aux traités et à la Charte des droits fondamentaux de l'Union.

Comme nous l'avons déjà analysé, la CJUE a considéré, dans son avis du 26 juillet 2017⁷⁸², que si le transfert, la conservation et l'utilisation systématique des données de dossiers passagers que prévoit l'accord PNR sont pour l'essentiel admissibles, plusieurs dispositions du projet ne sont pas conformes aux exigences découlant des droits fondamentaux de l'Union européenne⁷⁸³. Les juges de Luxembourg ont donc considéré que « l'accord PNR ne peut pas être conclu sous sa forme actuelle en raison de l'incompatibilité de plusieurs de ses dispositions avec les droits fondamentaux reconnus par l'Union »⁷⁸⁴.

Pourtant, le Conseil avait déclaré que l'équilibre entre la sécurité collective et la protection des droits fondamentaux était réalisé. En effet, dans un communiqué de presse diffusé le jour

⁷⁷⁹ Conseil de l'Union européenne, Communiqué de presse, « Signature de l'accord UE-Canada sur les données des dossiers passagers (données PNR), 25 juin 2014, Bruxelles, Presse.

⁷⁸⁰ Projet de décision du Conseil relative à la conclusion, au nom de l'Union, de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, 2013, (12652/2013).

⁷⁸¹ Accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, 2013, (12657/2013).

⁷⁸² D. SIMON, « Droit fondamentaux », *Europe*, octobre 2017, Commentaire n° 345, pp. 17-18 ; J. EYNARD, « D'une ingérence généralisée à une autre : deux poids, deux mesures ? », *Revue trimestrielle des droits de l'homme*, 2018, pp. 761-783.

⁷⁸³ CJUE, 26 juillet 2017, avis 1/15.

⁷⁸⁴ CJUE, Communiqué de presse n° 89/16, Conclusions de l'avocat général dans la demande d'avis 1/15, Luxembourg, le 8 septembre 2016.

de la signature de l'accord, le Conseil avait mis en avant les principaux éléments de l'accord parmi lesquels : a) une limitation stricte des finalités, l'utilisation des données PNR étant limitée à la prévention et à la détection d'infractions terroristes ou de formes graves de criminalité transnationale, ainsi qu'aux enquêtes et poursuites en la matière, b) l'obligation juridiquement contraignante, pour les autorités canadiennes, d'informer les États membres et les autorités de l'UE de toutes les pistes susceptibles d'intéresser l'UE qui découleraient de l'analyse de ces données PNR, c) un régime solide de protection des données assorti d'exigences strictes en matière de sécurité et d'intégrité des données et d'un masquage immédiat des données sensibles (qui ne peuvent être utilisées que lorsque cela s'avère indispensable, parce que la vie d'une personne est en danger ou qu'il existe un risque de blessure grave, d) des droits d'accès, de rectification et d'effacement, ainsi que la possibilité d'introduire un recours administratif ou judiciaire, e) une durée de stockage des données PNR limitée à cinq ans, après trente jours, le Canada est tenu de dépersonnaliser les données PNR par masquage des noms de tous les passagers et, après deux ans, il est tenu de masquer tous les éléments des données PNR pouvant donner lieu à l'identification des passagers⁷⁸⁵.

Mais cela n'a pas suffi à convaincre le Parlement qui s'est tout de même tourné vers la Cour de justice sachant que dans un arrêt rendu le 4 avril 2014, celle-ci a remis en cause la directive de 2006 sur la rétention des données. En outre, un avis critique du Contrôleur européen de la protection des données concernant la proportionnalité des systèmes PNR, le transfert massif de données et le choix de la base juridique pour l'accord, a encouragé les eurodéputés à demander l'avis des juges de Luxembourg⁷⁸⁶. La volonté du Conseil de l'Union européenne de se montrer comme un colégislateur à la recherche d'un équilibre entre les principes de sécurité et de liberté n'a donc pas convaincu.

Le contexte européen, avec plusieurs attentats qui ont touché l'Europe, a compliqué le dossier des accords PNR⁷⁸⁷ ; les attaques terroristes rendent la volonté de renforcer la sécurité collective encore plus pressante mais la défense des droits fondamentaux des citoyens, dont celui de la protection de la vie privée et des données personnelles, devient alors plus difficile à

⁷⁸⁵ Conseil de l'Union européenne, Communiqué de presse, « Signature de l'accord UE-Canada sur les données des dossiers passagers (données PNR), 25 juin 2014, Bruxelles, Presse.

⁷⁸⁶ F. MICHEA, « Les finalités des systèmes d'information européens à vocation migratoire », l'Union européenne et la tentation du panoptique, in S. TURGIS, *Les données numériques des migrants et des réfugiés sous l'angle du droit européen*, Presses universitaires de Rennes, 2020, pp. 37-63.

⁷⁸⁷ V. GAUTRON, D. MONNIAUX, « De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme », in *Archives de politique criminelle*, Terrorisme, Éditions Pédone, 2016, pp. 123-135. Voir aussi D. KORFF, M. GEORGES, *Passenger Name Records, data mining & data protection: the need for strong safeguards*, The Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 2015, p. 34.

porter sur la scène politique, car l'opinion publique est souvent traumatisée par les scènes de violence qu'elle perçoit. Par ailleurs, le départ des ressortissants européens vers la Syrie et d'autres zones de conflit au Moyen-Orient et en Afrique renforce les arguments en faveur d'accords PNR⁷⁸⁸.

Sous-section 2 – La Commission, l'organe négociateur des accords PNR

Symbole de la « méthode communautaire », la Commission européenne (ci-après la Commission) est une institution qui revêt un caractère *sui generis* car « elle n'a d'équivalent ni dans les ordres juridiques nationaux ni dans l'ordre juridique international »⁷⁸⁹. Cette spécificité rend difficile toute tentative de comparaison avec d'autres organes préexistants dans d'autres ordres juridiques. Certaines des attributions de la Commission permettent de la comparer à une administration internationale classique tandis que d'autres à un gouvernement étatique ; d'autres encore, à une autorité de régulation, à un ministère public ou à un corps diplomatique. Malgré cela, la Commission ne peut être réduite à un seul de ces organes cités.

§ 1 – La Commission, l'organe symbole de la méthode communautaire

Le traité sur l'Union européenne (ci-après TUE) classe la Commission européenne au titre des institutions de l'Union, à la suite du Parlement européen, du Conseil européen, et avant la Cour de justice de l'Union européenne, la Banque centrale européenne et la Cour des comptes⁷⁹⁰. La mission essentielle de cette institution, siégeant à Bruxelles et à Luxembourg, est de promouvoir l'intérêt général de l'Union et de prendre les initiatives appropriées à cette fin comme le rappelle l'article 17 du TUE qui ajoute, par ailleurs, que la Commission veille à l'application des traités ainsi qu'aux mesures adoptées par les institutions en vertu de ceux-ci. Elle surveille l'application du droit de l'Union sous le contrôle de la CJUE. Elle exécute le budget et gère les programmes. Elle exerce des fonctions de coordination, d'exécution et de gestion conformément aux conditions prévues par les traités⁷⁹¹. À l'exception de la politique étrangère et de sécurité commune, et des autres cas prévus par les traités, la Commission « assure la représentation extérieure de l'Union »⁷⁹². Par ailleurs, « elle prend les initiatives de la programmation annuelle et pluriannuelle de l'Union pour parvenir à des accords interinstitutionnels »⁷⁹³.

⁷⁸⁸ C. CALOTHY, « Face au terrorisme, progrès et limites d'une coopération internationale tous azimuts », *Pouvoirs*, La lutte contre le terrorisme, Le Seuil, 2016, pp. 125-137.

⁷⁸⁹ E. BERNARD, « Commission européenne », *Dalloz*, décembre 2019.

⁷⁹⁰ TUE, article 13.

⁷⁹¹ TUE, article 17.

⁷⁹² Ibidem

⁷⁹³ Ibid.

Les pères fondateurs du projet européen souhaitaient soumettre les États membres aux décisions d'une institution indépendante dans le but de réaliser « les premières assises concrètes d'une Fédération européenne indispensable à la préservation de la paix »⁷⁹⁴. Cette indépendance prendra la forme d'une « supranationalité » qui caractérise aujourd'hui l'originalité de la méthode communautaire⁷⁹⁵.

Outre, la proposition de nouveaux textes de loi, la gestion des politiques de l'UE et la veille au respect du droit européen, la Commission représente l'UE dans le monde. C'est dans ce cadre qu'elle négocie les accords internationaux engageant l'UE, dont l'accord PNR.

§ 2 – La négociation de l'accord international PNR

Le Traité de Lisbonne a modifié le droit européen relatif à la négociation des accords internationaux⁷⁹⁶. Avant la révision du Traité de Lisbonne, la négociation de ces accords relevait, dans le pilier communautaire, de la compétence de la Commission. Cette dernière se limitait à assister la présidence de l'Union, dans certains cas, lors des négociations d'accords relevant des deuxième et troisième piliers relatifs, respectivement, à la politique étrangère et de sécurité commune (PESC) et à la coopération dans les domaines de la justice et des affaires intérieures (JAI).

Depuis cette révision, le périmètre des prérogatives de la Commission en la matière a été réduit au bénéfice des compétences attribuées à un Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité. L'article 218 paragraphe 2⁷⁹⁷ du TFUE indique qu'il revient à la Commission ou au Haut représentant de l'UE de présenter des recommandations au Conseil lorsque l'accord envisagé porte « exclusivement ou principalement » sur la politique étrangère et de sécurité commune (ci-après) PESC. Elle vise principalement à coordonner les politiques étrangères des États membres, en favorisant les échanges d'informations, les consultations mutuelles entre gouvernements, ainsi que l'harmonisation des positions et des actions diplomatiques conjointes. L'objectif est de faire émerger des principes communs, accompagnés si nécessaire de mesures concrètes pour leur application⁷⁹⁸.

⁷⁹⁴ R. SCHUMAN, *Discours de l'horloge*, 9 mai 1950.

⁷⁹⁵ E. BERNARD, « Commission européenne », *Dalloz*, décembre 2019.

⁷⁹⁶ Ibidem

⁷⁹⁷ TFUE, article 218, paragraphe 2.

⁷⁹⁸ M. LEFEBVRE, *La politique étrangère européenne*, Presses universitaires de France, 2021. L'auteur insiste sur le caractère « ambivalent » de l'« action extérieure » de l'Union européenne du fait de la tension entre le respect de la souveraineté des États membres et de l'aspiration supranationale du projet européen.

Le Conseil prend une décision qui autorise l'ouverture des négociations et désigne, en fonction de la matière envisagée, « le négociateur ou le chef de l'équipe de négociation de l'Union ». Ce dernier peut être la Commission mais le droit européen ne lui garantit pas cette mission⁷⁹⁹. L'article 218 du TFUE rappelle que le Conseil « peut adresser des directives au négociateur et désigner un comité spécial, les négociations devant être conduites en consultation avec ce comité »⁸⁰⁰. Par ailleurs, l'alinéa suivant indique que la décision portant conclusion de l'accord relève de la compétence du Conseil « sur proposition du négociateur »⁸⁰¹.

Dans le cadre de l'accord avec les États-Unis, la Commission est intervenue de la façon suivante. Dès 2002, après avoir reconnu la légitimité des intérêts de sécurité, la Commission a informé les autorités américaines que leur nouvelle législation PNR pouvait entrer en conflit avec la législation européenne, et celle de ses États membres, en matière de protection des données personnelles. En 2003, elle a entamé des négociations avec les autorités américaines, lesquelles ont donné lieu à un document contenant des engagements pris par le Customs and Border Protection (CBP)⁸⁰² en vue de l'adoption, par la Commission, d'une décision d'adéquation sur la base de l'article 25 § 6 de la directive 95/46.

Le 1^{er} mars 2004, en vertu de l'article 25 § 6 de la directive, la Commission a saisi le Parlement européen du projet de décision d'adéquation assorti du projet d'engagements du CBP. Le 31 mars 2004, le Parlement a adopté une résolution faisant état d'un certain nombre de réserves d'ordre juridique sur la proposition qui lui avait été soumise en application de l'article 8 de la décision 1999/468/CE du Conseil du 28 juin 1999, fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission⁸⁰³. Dans cette résolution, il a considéré, en particulier, que le projet de décision d'adéquation excédait les compétences conférées à la Commission par l'article 25 de la directive. Le Parlement a appelé à la conclusion d'un accord international approprié respectant les droits fondamentaux sur un certain nombre de points détaillés dans ladite résolution et a demandé à la Commission de lui soumettre un nouveau projet de décision. Il s'est en outre réservé le droit de saisir la Cour, aux

⁷⁹⁹ E. BERNARD, « Commission européenne », *Dalloz*, décembre 2019.

⁸⁰⁰ TFUE, article 218, paragraphe 4.

⁸⁰¹ TFUE, article 218, paragraphe 5.

⁸⁰² La CBP est l'agence fédérale chargée de sécuriser les frontières des États-Unis et de faciliter le commerce ainsi que les déplacements légaux.

⁸⁰³ Résolution du Parlement européen sur le projet de décision de la Commission constatant le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (2004/2011(INI)), 31 mars 2004.

fins de vérifier la légalité de l'accord international envisagé et, en particulier, la compatibilité de celui-ci avec la protection du droit à la vie privée.

Le 14 mai 2004, la Commission a adopté la décision d'adéquation, qui fait l'objet de l'affaire C-318/04⁸⁰⁴. Puis, le 17 mai 2004, le Conseil a adopté la décision 2004/496, qui fait l'objet de l'affaire C-317/04⁸⁰⁵.

Le 30 mai 2006, la CJUE a annulé⁸⁰⁶, d'une part, la décision 2004/496/CE du Conseil du 17 mai 2004 concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la Sécurité intérieure et, d'autre part, la décision 2004/535/CE de la Commission du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique. Les effets de la décision 2004/535 ont été maintenus jusqu'au 30 septembre 2006.

Dans le contexte suivant les attentats du 11 septembre 2001, la Commission n'a pas été en mesure d'imposer, avec fermeté, la défense du modèle européen de protection des données personnelles que le groupe 29 avait mis en avant dans ses recommandations, notamment dans son appel au respect du principe de proportionnalité et la condamnation du système « pull »⁸⁰⁷. Elle s'est finalement contentée de son rôle exécutif au sein de l'Union européenne dans un contexte politique où l'intérêt général de l'Union européenne semblait être ciblée sur la protection collective de la sécurité des européens⁸⁰⁸.

Dans le cadre de l'accord PNR avec le Canada, les mêmes hésitations ont marqué la signature de l'accord PNR entre les deux parties⁸⁰⁹. Toutefois, puisque la négociation s'est tenue après le Traité de Lisbonne, les accords ont été négociés par le Haut représentant en matière de politique étrangère et de sécurité, excluant donc la Commission de la négociation.

⁸⁰⁴ Commission européenne, Décision d'adéquation du 14 mai 2004, affaire C-318/04.

⁸⁰⁵ Conseil de l'Union européenne, Décision 2004/496 du 17 mai 2004, dans l'affaire C-317/04.

⁸⁰⁶ CJUE, 30 mai 2006, aff. C-317/04 et C-318/04, Parlement européen c/ Conseil de l'Union européenne.

⁸⁰⁷ V. MICHEL, « La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration », *Revue trimestrielle de droit européen*, Dalloz, 2006.

⁸⁰⁸ E. DUBOUT, « Principes, droits et devoirs dans la Charte des droits fondamentaux de l'Union européenne », *RTDE*, Dalloz, 2014, p. 409 et s.

⁸⁰⁹ C. RAPOPORT, « Chronique Action extérieure de l'Union européenne - Avis 1/15 relatif à l'accord PNR UE-Canada : la Cour murmure à l'oreille du négociateur et du législateur ! », *RTDE*, Dalloz, 2018, p. 201.

Le 18 juillet 2005⁸¹⁰, le Conseil de l'UE a adopté la décision 2006/230/CE relative à la conclusion de l'accord entre la Communauté européenne et le Gouvernement du Canada sur le traitement des données des passagers aériens, dont l'Information préalable sur les voyageurs et le dossier passager (ci-après IPV/DP). Ces données permettent à l'Agence des services frontaliers du Canada (ASFC) « d'effectuer une évaluation du risque sur les voyageurs et les membres d'équipage pendant qu'ils sont en route vers le Canada »⁸¹¹. D'après le préambule, cet accord a été conclu au vu de « l'obligation imposée par le gouvernement du Canada aux transporteurs aériens de passagers vers le Canada de fournir aux autorités canadiennes compétentes des données relatives aux informations préalables sur les voyageurs et aux dossiers passagers (ci-après dénommées "IPV/DP»), dans la mesure où elles sont recueillies et stockées dans leurs systèmes de réservation automatisés et systèmes de contrôle des départs »⁸¹².

En vertu de l'article 1^{er}, paragraphe 1, de l'accord de 2006, celui-ci avait « pour objet d'assurer que les données IPV/DP des personnes effectuant des voyages admissibles [soient] fournies dans le plein respect des droits et des libertés fondamentaux, et notamment le droit au respect de la vie privée »⁸¹³. Selon l'article 3, paragraphe 1, de cet accord, les « [p]arties [étaient convenues] que les données IPV/DP des personnes effectuant des voyages admissibles [soient] traitées comme énoncé dans les engagements pris par l'autorité compétente obtenant les données IPV/DP ». L'autorité compétente pour le Canada était, conformément à l'annexe I dudit accord, l'ASFC⁸¹⁴.

Sur la base de ces engagements, la Commission a adopté, le 6 septembre 2005, la décision 2006/253/CE constatant le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférées à l'ASFC⁸¹⁵. L'article 1^{er} de cette décision prévoyait qu'« [a]ux fins de l'article 25, paragraphe 2, de la directive [95/46], l'[ASFC] est considérée comme assurant un niveau de protection adéquat des données DP transférées de la Communauté en ce qui concerne les vols à destination du Canada, conformément aux [engagements de l'ASFC concernant son programme DP] figurant à

⁸¹⁰ CJUE, 26 juillet 2017, avis 1/15.

⁸¹¹ Agence des services frontaliers du Canada, L'information préalable sur les voyageurs et le dossier passager https://cbsa-asfc.gc.ca/security-securite/api_ipv-fra.html. Sur l'accord PNR entre l'Union européenne et le Canada, voir aussi R. TINIÈRE (dir.), « Droit fondamentaux », in *Annuaire de droit de l'Union européenne*, Éditions Panthéon-Assas, 2020.

⁸¹² CJUE, 26 juillet 2017, avis 1/15.

⁸¹³ Ibidem

⁸¹⁴ Ibid.

⁸¹⁵ JO 2006, L 91, p. 49.

l'annexe » de ladite décision⁸¹⁶. En vertu de son article 7, cette même décision prévoyait qu'elle « viendra[it] à échéance trois ans et six mois à compter de sa notification, à moins qu'elle ne soit prolongée conformément à la procédure prévue à l'article 31, paragraphe 2, de la directive [95/46] »⁸¹⁷. Une telle prolongation ne s'est pas réalisée. La durée de validité de l'accord étant, conformément à son article 5, paragraphes 1 et 2, liée à celle de la décision 2006/253, ledit accord est venu à échéance au mois de septembre 2009. Cette séquence illustre l'approche accommodante de la Commission lorsqu'elle a évalué le niveau d'adéquation de l'accord PNR avec les standards de protection afin de favoriser la conclusion d'un accord renforçant ainsi la sécurité collective.

Le 2 décembre 2010, le Conseil a adopté une décision ainsi que des directives de négociation qui ont autorisé la Commission à ouvrir des négociations avec le Canada, au nom de l'Union européenne, en vue d'un accord sur le transfert et l'utilisation des données PNR destiné à prévenir et à combattre le terrorisme et les autres formes graves de criminalité transnationale.

Issu de ces négociations avec le Canada, un accord a été paraphé le 6 mai 2013. Puis, le 18 juillet 2013, la Commission a adopté deux propositions de décisions du Conseil relatives, pour l'une, à la conclusion de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers et, pour l'autre, à la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers⁸¹⁸.

Le Contrôleur européen de la protection des données a émis un avis, le 30 septembre 2013, sur ces propositions de décisions⁸¹⁹. Le 5 décembre 2013, le Conseil a adopté la décision relative à la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers⁸²⁰. Le même jour, le Conseil a décidé que l'approbation du Parlement serait sollicitée sur son projet de décision relative à la conclusion de l'accord envisagé. L'accord envisagé a été signé le 25 juin 2014.

Le 7 juillet 2014, le Conseil, par lettre, a demandé au Parlement d'approuver le projet de décision du Conseil relative à la conclusion de l'accord PNR. Plusieurs mois plus tard, le

⁸¹⁶ CJUE, 26 juillet 2017, avis 1/15.

⁸¹⁷ Ibidem

⁸¹⁸ S. PEYROU, « La protection des données personnelles face aux programmes PNR. Une illustration du difficile équilibre entre lutte contre le terrorisme et protection des droits fondamentaux », in *Mélanges en l'honneur du Professeur Pierre Bon*, Dalloz, 2014, pp. 496-497.

⁸¹⁹ Avis du CEPD du 30 septembre 2013 sur les propositions de décisions du Conseil relatives à la conclusion et à la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, JOUE 2014 C 51.

⁸²⁰ Décision du 5 décembre 2013 relative à la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers.

Parlement a adopté, le 25 novembre 2014, la résolution sur la saisine, pour avis, de la Cour de justice à propos de la compatibilité avec les traités de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers⁸²¹. Le 26 juillet 2017, la Cour de justice a jugé que cet accord ne pouvait pas être adopté dans sa forme actuelle en raison de l'incompatibilité de plusieurs de ses dispositions avec les droits fondamentaux reconnus par l'Union européenne⁸²².

Dans le cadre de ses prérogatives de surveillance et de contrôle, le rôle de la Commission est, selon l'énoncé traditionnel, celui d'une « gardienne » des traités et de la légalité communautaire⁸²³. Cette dernière a pour mission, en effet, de veiller à l'application des traités ainsi que des mesures adoptées par les institutions en vertu de ceux-ci ainsi que de surveiller « l'application du droit de l'Union sous le contrôle de la Cour de justice »⁸²⁴. Cette méthode communautaire a pour conséquence, dès le début, que la mission de surveillance et de contrôle du droit de l'Union – comprenant les traités, les accords internationaux auxquels l'Union est partie, du droit dérivé et, désormais, de la Charte des droits fondamentaux – soit confiée à un organe indépendant des États membres. Cette mission revient donc naturellement à la Commission⁸²⁵. Afin de la mener à bien, cette dernière bénéficie des pouvoirs d'information, de prévention et d'investigation qu'elle exerce en formulant des avis et des recommandations⁸²⁶. Par ailleurs, la Commission peut poursuivre les infractions au droit de l'Union.

Ainsi, dans les négociations que la Commission a menées, il semble que la mission de contrôle du droit de l'Union, notamment le respect des droits fondamentaux dont ceux de la protection de la vie privée et des données à caractère personnel, n'a pas été effective comme les arrêts de la Cour de justice à ce sujet le rappelleront. La Commission n'a finalement été qu'un organe de négociation, agissant sous le mandat du Conseil vis-à-vis des parties nord-américaines dont l'objectif était d'assurer la réalisation d'un accord visant avant tout et surtout à mener une « lutte efficace contre le terrorisme et la criminalité organisée »⁸²⁷.

⁸²¹ Résolution du Parlement européen du 25 novembre 2014 sur la saisine pour avis de la Cour de justice sur la compatibilité avec les traités de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers (2014/2966(RSP)).

⁸²² CJUE, 26 juillet 2017, avis 1/15.

⁸²³ E. BERNARD, « Commission européenne », *Dalloz*, décembre 2019.

⁸²⁴ TUE, article 17, § 1^{er}.

⁸²⁵ E. BERNARD, « Commission européenne », *Dalloz*, décembre 2019.

⁸²⁶ *Ibidem*

⁸²⁷ L'Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers ("données PNR") par les transporteurs aériens au ministère américain de la sécurité intérieure ("DHS") (accord PNR 2007) 11595/07 du 18 juillet 2007.

Motivé par des considérations politiques, ce choix en faveur de la sécurité publique a une incidence négative sur l'adéquation des accords internationaux aux standards de protection des données personnelles sur lesquels doit veiller la Commission et, par ricochet, sur la protection de la légalité communautaire. En effet, il rend plus difficile la protection des données personnelles des passagers aériens, car il relègue cette protection des droits individuels au profit de la sécurité publique en abaissant les exigences des institutions européennes vis-à-vis de l'adéquation des accords PNR aux standards européens.

§ 3 – L'illustration du pouvoir d'initiative de la Commission au sujet de la directive PNR

Reconnue comme « moteur de l'intégration », la Commission dispose d'un pouvoir d'initiative qui est sa prérogative principale. L'article 17, paragraphe 2, du Traité de l'Union Européenne prévoit qu'« un acte législatif de l'Union ne peut être adopté que sur proposition de la Commission, sauf dans les cas où les traités en disposent autrement. Les autres actes sont adoptés sur proposition de la Commission lorsque les traités le prévoient ». Ce pouvoir lui laisse la plus grande liberté et lui confère l'essentiel de sa dimension politique⁸²⁸. En effet, la Commission a un droit de proposition quasi exclusif dans le cadre du processus décisionnel de l'Union européenne. Toutefois, l'attribution d'un tel pouvoir à un organe dont les membres n'ont pas été élus fait l'objet de critiques⁸²⁹. Pour certains, l'octroi de ce pouvoir contribue à creuser le déficit démocratique dont souffre le projet communautaire puisque, dans les États démocratiques, l'initiative des actes législatifs revient généralement aux parlements et aux gouvernements. Or, la transposition des schémas nationaux au niveau de l'Union est imparfaite⁸³⁰. Ce pouvoir d'initiative, qui s'ajoute au rôle de la Commission en tant que force d'impulsion, est plus large puisque la Commission est chargée de promouvoir l'intérêt général de l'Union et de prendre « les initiatives » appropriées à cette fin, tel qu'il est énoncé dans l'article 17, paragraphe 1 du TUE. La Commission élabore et présente au Conseil et au Parlement toutes les propositions législatives, les règlements ou directives, nécessaires pour appliquer les traités.

Cependant, ce monopole de la Commission présente des limites comme c'est le cas en matière de liberté, de sécurité et de justice, où il existe un droit ne pouvant être exercé que collectivement par un quart des États membres. Dans ces domaines particuliers, la Commission européenne a le pouvoir exclusif d'agir, mais qu'il existe des cas où cette

⁸²⁸ E. BERNARD, « Commission européenne », *Dalloz*, décembre 2019.

⁸²⁹ *Ibidem*

⁸³⁰ *Ibid.*

exclusivité est limitée et où une action collective impliquant au moins un quart des États membres est nécessaire pour exercer certains droits ou prendre certaines décisions.

Par ailleurs, ce pouvoir d'initiative, lorsque la Commission l'exerce, peut être soumis à diverses contraintes ou influences qui peuvent être d'ordre politique ou juridique⁸³¹. D'une part, la Commission peut subir l'influence des États membres lorsqu'elle est appelée à s'aligner sur les préoccupations nationales, puisqu'elle est amenée à consulter divers experts et organismes nationaux dans le cadre de l'élaboration de sa proposition⁸³². En effet, la Commission augmente ses chances de voir sa proposition adoptée par le Conseil, lors du vote, lorsqu'elle s'assure du soutien des États. Toutefois, la Commission prend « le risque de se détourner de l'objectif de l'Union pour la quête d'intérêts nationaux subjectifs »⁸³³, privilégiant ainsi « le possible au souhaitable »⁸³⁴.

Dans le cadre la directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, la Commission a joué un rôle d'initiative. La Commission a adopté, le 6 novembre 2007, une proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers à des fins répressives⁸³⁵. Cette dernière a fait l'objet de « discussions approfondies » au sein des groupes de travail du Conseil de l'Union européenne. Après l'entrée en vigueur du TFUE, le 1^{er} décembre 2009, cette proposition de la Commission est devenue obsolète. D'ailleurs, elle n'avait pas été encore adoptée par le Conseil⁸³⁶.

Le 4 février 2011, la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers 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, a remplacé la proposition de 2007. La nouvelle proposition de 2011 reposait sur les dispositions du TFUE et tenait compte des recommandations émises par le Parlement dans sa résolution de 2008⁸³⁷. Cette proposition de 2011 traduisait ainsi « un état

⁸³¹ Ibid.

⁸³² P. PONZANO, « Le droit d'initiative législative de la Commission européenne : théorie et pratique », *Revue des affaires européennes*, n° 1, 2009.

⁸³³ E. BERNARD, « Commission européenne », *Dalloz*, décembre 2019.

⁸³⁴ D. SIMON, *Le système juridique communautaire*, 3e éd., Paris, PUF, 2001, p. 198.

⁸³⁵ Conseil de l'Union européenne, Proposition de Directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers 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, n° 6007/11, Bruxelles, le 4 février 2011.

⁸³⁶ Ibidem

⁸³⁷ Ibid.

d'avancement des discussions au sein du groupe de travail du Conseil en 2009 »⁸³⁸ et prenait en compte les avis formulés par le Contrôleur européen de la protection des données⁸³⁹, de l'Agence des droits fondamentaux⁸⁴⁰ et du groupe « article 29 » sur la protection des données⁸⁴¹.

Après plusieurs essais ayant échoué au Parlement européen, la directive 2016/681 du Parlement européen et du Conseil 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, fut finalement adoptée le 27 avril 2016, en même temps que le RGPD.

Section 2 – Des acteurs garants des droits fondamentaux des passagers aériens : le Parlement européen, la Cour de justice de l'Union européenne, le Comité européen de la protection des données et le Contrôleur européen de la protection des données

Soumis à des pressions politiques, le Parlement européen (sous-section 1), la Cour de justice (sous-section 2), le Comité européen de la protection des données (sous-section 3) et le Contrôleur européen de la protection des données (sous-section 4) ont cependant développé les initiatives nécessaires pour trouver un équilibre entre le renforcement de la sécurité et la sauvegarde des droits fondamentaux des citoyens européens, dont la protection des données personnelles.

Sous-section 1 – Le Parlement européen, une institution impliquée dans la protection des droits fondamentaux

Composée des représentants des citoyens de l'Union, le Parlement européen partage les compétences budgétaires et législatives avec le Conseil de l'Union européenne. Parmi les principales institutions, le Parlement est celle qui a mis le plus en avant la protection des données personnelles des passagers aériens.

⁸³⁸ Ibid.

⁸³⁹ C. DE TERWANGNE, K. ROSIER (dir.), « Des lignes directrices du Groupe de l'article 29 aux travaux (futurs) du Comité européen de la protection des données (CEPD) in *Le règlement général sur la protection des données (RGPD, GDPR)*, Larcier, 2018.

⁸⁴⁰ Créée en 2007, l'Agence des droits fondamentaux a pour mission de fournir des conseils indépendants sur la protection des droits fondamentaux, sur la base d'éléments factuels, à destination des décideurs européens et ceux des États membres. Voir A-M. OLIVA, « Les agences de l'Union européenne, in *Les indispensables du droit des institutions européennes*, Ellipses, 2016, pp. 178-183.

⁸⁴¹ J-P. JACQUÉ, « Parlement européen », in *Répertoire de droit européen*, Dalloz, 2020. Voir aussi. Avis n°145 du 5 décembre 2007 du Parlement européen.

§ 1 – Le Parlement européen, une institution associant les citoyens à la construction européenne

Le Parlement européen se distingue des autres institutions européennes par une histoire marquée par l'extension progressive de ses pouvoirs. Au début de la construction européenne, les articles 20 et suivants du Traité instituant la Communauté européenne du charbon et de l'acier (CECA) avaient établi une Assemblée « composée des représentants des peuples des États réunis dans la Communauté »⁸⁴², à laquelle ils octroyaient un pouvoir de contrôle. Cette formule excluait toute référence aux citoyens ou peuples européens dès lors que n'étaient visés que les peuples des États⁸⁴³. La doctrine en a conclu que cette assemblée instituée par le traité ne bénéficiait pas d'une légitimité démocratique directe mais indirecte au travers des peuples des États membres. Les révisions des traités européens, ceux d'Amsterdam et de Lisbonne notamment, ont fini par faire du Parlement européen une « assemblée unique » figurant parmi les institutions de l'Union européenne⁸⁴⁴. Ainsi, les pouvoirs du Parlement – reconnus par le droit européen – ont été précisés par la voie d'accords avec les autres institutions et ont été accrus par les révisions successives des traités. Avec le Traité sur l'Union européenne, la Conférence intergouvernementale sur l'Union politique a consacré un accroissement des pouvoirs de l'institution parlementaire tant sur le plan législatif que sur celui du contrôle. Concluant cette évolution, le Traité de Lisbonne a fait de la procédure de codécision la procédure législative de droit commun⁸⁴⁵.

La composition du Parlement européen⁸⁴⁶ est prévue par l'article 14 du Traité sur l'Union européenne qui fixe des critères en la matière. Ce dernier prévoit notamment que les représentants des citoyens de l'Union européenne ne peuvent pas être plus de sept cent cinquante, plus le président. Par ailleurs, il est indiqué que la représentation doit être assurée de façon dégressivement proportionnelle. Ainsi, la loi fixe un seuil minimal de six membres par État membre. Conséquemment, aucun État membre de l'Union ne peut se voir attribuer plus de quatre-vingt-seize sièges.

⁸⁴² Traité instituant la Communauté Européenne du Charbon et de l'Acier, 18 avril 1951, Paris.

⁸⁴³ J.-P. JACQUÉ, « Parlement européen », in *Répertoire de droit européen*, Dalloz, 2020.

⁸⁴⁴ Ibidem

⁸⁴⁵ Ibid.

⁸⁴⁶ V. DEMERTZIS, « Élire le Parlement européen », *Courrier hebdomadaire du CRISP*, 2014, pp. 5-100. Voir aussi B. CASSEN, H. MICHEL, L. WEBER, *Le Parlement européen, pour faire quoi ?*, Brignais, Éditions du Croquant, 2014 ; O. COSTA, *Le Parlement européen, assemblée délibérante*, Bruxelles, Éditions de l'Université de Bruxelles, 2001.

Depuis 2014, le Parlement européen était composé de 751 députés élus dans les vingt-huit États membres de l'Union européenne⁸⁴⁷. Toutefois, le Parlement européen est passé de 751 à 705 députés depuis que le Royaume-Uni a quitté l'Union européenne en 2020. Depuis 1979, les députés européens sont élus au suffrage universel direct pour une durée de cinq ans. Par ailleurs, chaque pays détermine son propre mode de scrutin. Quant aux sièges, ils sont attribués en fonction du nombre d'habitants de chaque État membre⁸⁴⁸.

Dans le règlement intérieur du Parlement européen⁸⁴⁹, son organisation et son fonctionnement sont précisés. Son président est élu pour un mandat de deux ans et demi renouvelables, soit une demi-législature. Les députés européens siègent au sein de groupes politiques transnationaux qui sont constitués par affinités politiques.

Le Parlement européen est composé de vingt commissions permanentes dont la fonction est d'examiner les textes avant leur discussion⁸⁵⁰. Les députés européens se réunissent le deuxième mardi du mois de mars et tiennent une session annuelle. La session annuelle correspond à une période d'un an tandis que le terme de « période de session » renvoie à la réunion que tient le Parlement, en règle générale, chaque mois. À la demande de la majorité de ses membres, du Conseil ou de la Commission, le Parlement se réunit en session extraordinaire.

La Conférence des présidents des groupes politiques prépare l'ordre du jour, que le Parlement adopte ensuite. Le vote a lieu à la majorité absolue et le quorum est fixé au tiers des membres du Parlement. Toutefois, en pratique, cette règle n'est pas respectée. En principe, les votes se font à main levée mais peuvent également avoir lieu sous forme électronique ou au scrutin secret.

Le Règlement intérieur du Parlement européen prévoit des privilèges et des immunités pour les parlementaires⁸⁵¹ dont le statut unique instaure des dispositions communes à tous les parlementaires. Certaines immunités sont prévues notamment quant aux votes et opinions émis ou des incompatibilités avec les fonctions de membre d'un gouvernement, de la Commission, de la Cour de justice de l'Union européenne ou de la Cour des comptes. Par ailleurs, des incompatibilités peuvent être prévues par les législations nationales.

⁸⁴⁷ *Parlement européen*, Fiche d'orientation, Dalloz, juin 2020. Voir D. NAZET ALLOUCHE, « Politique sociale – acteurs », in *Répertoire de droit européen*, Dalloz, 2019. Voir aussi X. DELPECH, « La directive PNR confrontée au respect des droits fondamentaux », Dalloz, 2022.

⁸⁴⁸ *Ibidem*

⁸⁴⁹ Règlement intérieur du Parlement européen, Parlement européen, juillet 2022.

⁸⁵⁰ Règlement intérieur du Parlement, article 38 et suivants.

⁸⁵¹ Règlement intérieur du Parlement, article 5.

Le Parlement européen détient trois types de compétences : législatives, budgétaires et de contrôle de l'exécutif de l'Union européenne. Dans le cadre ses compétences législatives, le Parlement participe, avec le Conseil à l'adoption des actes juridiques. Plusieurs modes de délibérations existent dans lesquels le Parlement est investi à différents degrés.

La première, la consultation, qui est une procédure législative spéciale dans laquelle le Conseil doit obligatoirement consulter le Parlement bien que son avis ne le lie pas⁸⁵². Cette consultation contribue à l'équilibre institutionnel. Dans ce cas, le Parlement doit statuer dans un délai raisonnable. L'avis du Parlement est requis dans différents domaines, comme les modalités d'exercice des droits liés à la citoyenneté européenne, en matière fiscale et monétaire, pour certains accords internationaux, la révision des traités ou en matière de politique étrangère et de sécurité commune.

La deuxième, la coopération, est une procédure introduite par l'Acte unique qui revêt un intérêt historique⁸⁵³. Elle offre la possibilité d'un dialogue entre le Parlement et le Conseil. Toutefois, en cas de désaccord en deuxième lecture, le Conseil devra statuer à l'unanimité.

La troisième, l'approbation, est également une procédure législative spéciale⁸⁵⁴. Il s'agit d'un droit de veto que détient le Parlement à l'égard d'une mesure envisagée par le Conseil. Cette procédure a été particulièrement utilisée en matière d'accords externes. Elle s'applique également pour l'adoption d'actes internes à l'Union, notamment aux décisions à caractère constitutionnel.

La quatrième, la procédure législative ordinaire, est une procédure de codécision mise en place avec le Traité de Maastricht dont le champ d'application s'est étendu de manière considérable⁸⁵⁵. Elle constitue aujourd'hui la procédure de droit commun. Cette procédure, régie par l'article 294 du TFUE, permet l'adoption d'actes pris conjointement entre le Parlement et le Conseil, après proposition de la Commission.

Outre ses compétences législatives, le Parlement dispose de compétences budgétaires qui lui permettent, avec le Conseil, d'établir le budget de l'Union européenne. Le Parlement a vu ses pouvoirs dans ce domaine s'accroître en matière de dépenses.

Enfin, le Parlement tient des compétences de contrôle de l'exécutif de l'Union européenne puisqu'il élit le président de la Commission. De plus, le choix des membres de la Commission

⁸⁵² Parlement européen, *Fiche d'orientation*, Dalloz, juin 2020.

⁸⁵³ Ibidem

⁸⁵⁴ Ibid.

⁸⁵⁵ Ibid.

est soumis à son approbation. Il peut également soumettre des questions au Conseil et à la Commission. Par ailleurs, il peut recevoir des pétitions de citoyens ou constituer des commissions temporaires d'enquête et dispose d'un droit d'action devant la Cour de justice.

§ 2 – Le Parlement européen, une institution communautaire de contrepoids pour la protection des données personnelles

Les institutions européennes ont pris conscience que face à la multiplication des échanges et de l'internationalité des parties prenantes, seule une action à l'échelon européen pouvait permettre la protection des données personnelles des citoyens européens. Le Parlement européen, contrairement au Conseil et à la Commission, s'est nettement distingué à ce sujet dans son action lors des négociations entre les Européens et leurs homologues américains et canadiens. Ce dernier a pu mettre en avant l'article 16 du TFUE qui garantit un droit à la protection des données personnelles à toute personne ainsi que les articles 7 et 8 de la Charte des droits fondamentaux qui garantissent le respect de la vie privée et la protection des données personnelles. En effet, le Parlement, conscient des enjeux actuels en la matière, a développé des initiatives pour rechercher l'équilibre entre le renforcement de la sécurité et la sauvegarde des droits fondamentaux⁸⁵⁶.

Tout d'abord, grâce à la procédure ordinaire de codécision, le Parlement européen peut concevoir des règles sur la protection des données personnelles. En effet, avec le Conseil, le Parlement européen élabore et adopte la législation européenne en matière de protection des données personnelles. À ce titre, le RGPD a permis au Parlement européen, et à d'autres institutions, d'instaurer un cadre général qui permet la protection des données personnelles dans l'espace communautaire. D'une part, il confère de nouveaux droits aux citoyens européens et, d'autre part, il s'applique directement dans l'ordre juridique des États membres puisqu'il s'agit d'un règlement. Il confère ainsi aux citoyens européens un arsenal juridique qu'ils peuvent opposer aux entreprises et à l'administration étatique⁸⁵⁷.

S'agissant de la protection des données personnelles des passagers aériens, le Parlement européen a clairement exprimé son désaccord à l'égard de certaines mesures mises en avant par la Commission européenne lors de la proposition de directive de 2013 permettant l'utilisation des données des dossiers passagers aériens pour la prévention et la détection des infractions terroristes et autres formes graves de criminalité, ainsi que pour les enquêtes et les

⁸⁵⁶ A. PETEL, « Le rôle du parlement européen dans la protection des données personnelles », Les Surligneurs, 24 mai 2019, en ligne à URL : <https://www.lesurligneurs.eu/le-role-du-parlement-europeen-dans-la-protection-des-donnees-personnelles/> consulté en ligne le 29 mars 2023.

⁸⁵⁷ CNIL, « Le Règlement général sur la protection des données – RGPD », 28 mai 2018.

poursuites en la matière⁸⁵⁸. Les eurodéputés avaient alors voté contre cette proposition en considérant que celle-ci était disproportionnée et nettement attentatoire aux droits fondamentaux. Toutefois, la vague d'attentats qui a visé les villes européennes début 2015 a marqué un tournant. C'est pourquoi le Parlement a revu sa position et négocié un compromis avec le Conseil pour adopter une directive en 2016⁸⁵⁹.

Puis, le Parlement a maintes fois exprimé sa position de défense de la protection des données personnelles des citoyens, à travers différentes résolutions. Ces dernières sont des actes juridiques non contraignants qui expriment la position d'une institution de l'Union européenne sur un problème juridique donné⁸⁶⁰.

Dans le cadre des négociations entre Européens et Américains sur un accord PNR, le Parlement a adopté une résolution, le 31 mars 2004⁸⁶¹, faisant état d'un certain nombre de réserves sur la proposition qui lui avait été soumise⁸⁶². Dans ce texte, les eurodéputés ont appelé à la conclusion d'un accord international approprié respectant les droits fondamentaux sur un certain nombre de points détaillés dans ladite résolution et ont demandé à la Commission de leur soumettre un nouveau projet de décision. Le Parlement s'était en outre réservé le droit de saisir la Cour aux fins de vérifier la légalité de l'accord international envisagé et, en particulier, la compatibilité de celui-ci avec la protection du droit à la vie privée.

Dans le cadre des négociations entre Européens et Canadiens sur l'accord PNR, le Conseil avait sollicité l'approbation du Parlement sur son projet de décision relative à la conclusion de l'accord envisagé. Ce dernier a été signé le 25 juin 2014 et, un mois plus tard, le 7 juillet 2014, le Conseil a demandé au Parlement, par lettre, d'approuver le projet de décision du Conseil relative à la conclusion de l'accord. Plusieurs mois plus tard, le 25 novembre 2014, le Parlement a adopté la résolution sur la saisine de la Cour de justice, pour avis, à propos de la

⁸⁵⁸ Parlement européen, « Rapport A7-0150/2013, Rapport sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers 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 », *Union européenne*, 29 avril 2013.

⁸⁵⁹ A. PETEL, « Le rôle du parlement européen dans la protection des données personnelles », *Les Surligneurs*, 24 mai 2019, en ligne à URL : <https://www.lesurligneurs.eu/le-role-du-parlement-europeen-dans-la-protection-des-donnees-personnelles/> consulté en ligne le 29 mars 2023.

⁸⁶⁰ Ibidem

⁸⁶¹ Résolution du Parlement européen sur le projet de décision de la Commission constatant le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (2004/2011(INI)), 31 mars 2004.

⁸⁶² V. BAZZOCCHI, « L'accord entre l'Union européenne et les États-Unis sur les données PNR », *European rights*, 2007, en ligne à URL : http://www.europeanrights.eu/public/commenti/Commento_Valentina_Bazzocchi_Accordo_PNR.pdf consulté le 29 mars 2023.

compatibilité de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers avec les traités européens. Puis, le 26 juillet 2017, la Cour de justice a affirmé dans un avis très commenté que cet accord ne pouvait pas « être conclu sous sa forme actuelle en raison de l'incompatibilité de plusieurs de ses dispositions avec les droits fondamentaux reconnus par l'Union [européenne] »⁸⁶³.

Sur un autre sujet de désaccord entre Européens et Nord-américains, le Parlement a adopté une résolution, le 12 mars 2014⁸⁶⁴, relative au programme de surveillance de l'Agence américaine de sécurité nationale sur les organismes de surveillance de plusieurs États membres et leurs incidences sur les droits fondamentaux des citoyens de l'Union européenne et sur la coopération transatlantique dans le domaine de la justice et des affaires intérieures. Cette résolution est la conséquence d'une enquête de six mois, menée par des députés européens, sur le sujet de la surveillance électronique de masse des citoyens européens. Cette enquête a été initiée à la suite des révélations de juin 2013 concernant l'espionnage auquel se seraient livrés les États-Unis et certains pays de l'Union.

Le Parlement a ainsi salué les efforts fournis pour améliorer le bouclier de protection des données (« Privacy Shield »), issu d'un accord de février 2016 entre l'Union européenne et les États-Unis sur les échanges de données transatlantiques, et repris dans la résolution du 26 mai 2016 sur les flux transatlantiques de données personnelles⁸⁶⁵. Ce mécanisme permet que les données personnelles des citoyens de l'Union européenne, transmises à des entreprises américaines, soient soumises à des règles qui assurent un niveau de protection adéquat et similaire à celui proposé par l'Union européenne.

Toutefois, le 16 juillet 2020, sur l'affaire dite « Schrems II », la CJUE a rendu un arrêt majeur concernant le régime de transferts de données entre l'Union européenne et les États-Unis⁸⁶⁶. Les juges de Luxembourg ont invalidé la décision d'adéquation « Privacy Shield », adoptée en 2016 par la Commission européenne à la suite de l'invalidation du « Safe Harbor », qui permettait le transfert de données entre l'Union européenne et les opérateurs américains adhérant à ses principes de protection des données sans autre formalité. La Cour de justice a

⁸⁶³ CJUE, Avis 1/15, Avis de la Cour, 26 juillet 2017.

⁸⁶⁴ Parlement européen, Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, Les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures, le 12 mars 2014.

⁸⁶⁵ A. PETEL, « Le rôle du parlement européen dans la protection des données personnelles », Les Surligneurs, 24 mai 2019, en ligne à URL : <https://www.lesurligneurs.eu/le-role-du-parlement-europeen-dans-la-protection-des-donnees-personnelles/> consulté en ligne le 29 mars 2023.

⁸⁶⁶ Cour de justice de l'Union européenne, Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems, Affaire C-311/18, 16 juillet 2020.

également invalidé les clauses contractuelles types permettant le transfert de données depuis l'Union européenne vers des importateurs établis hors de l'Union.

Le 25 mars 2022, l'Union européenne et les États-Unis ont trouvé un accord de principe sur le transfert des données transatlantiques, qui se voulait être « un équilibre entre la sécurité et le droit à la vie privée et à la protection des données »⁸⁶⁷. Cette annonce a rapidement été suivie d'une déclaration du CEPD qui a rappelé que sa consultation est obligatoire, sur le fondement de l'article 64 du RGPD, avant toute décision de la part de la Commission⁸⁶⁸. Cet accord de principe a été accompagné, le 7 octobre 2022, de la signature par Joe Biden d'un décret exécutif sur le renforcement des garanties en faveur des activités de renseignement lors de la transmission depuis des États-Unis⁸⁶⁹. Il applique le droit américain à tous les engagements pris en mars de la même année.

Le Parlement était également intervenu dans les débuts autour de la réforme d'Europol. Cette Agence de coopération policière de l'Union européenne a pour objectif de soutenir les États membres dans leur lutte contre la grande criminalité internationale et le terrorisme⁸⁷⁰. Le Parlement soutenait le renforcement des pouvoirs de l'agence européenne, considérant que Europol pouvait continuer à mener des projets de recherche et recevoir des données d'entreprises privées, tout en relevant que l'agence devait créer un nouveau poste d'officier aux droits fondamentaux et que le Contrôleur européen de la protection des données devait surveiller le traitement de données par Europol.

Le Parlement européen a également lancé des enquêtes pour examiner d'éventuelles violations du droit de l'Union européenne en matière de protection des données personnelles. Conformément à son pouvoir, il peut, à l'initiative d'un quart de ses membres, établir une commission d'enquête pour analyser les allégations de violations ou de mauvaise administration concernant l'application du droit européen. Cette compétence s'applique exclusivement aux actions des organes ou institutions de l'Union européenne, des

⁸⁶⁷ J. CHEMINAT, « USA et UE signent un accord pour succéder au Privacy Shield », Le monde informatique, 28 mars 2022, en ligne à URL : <https://www.lemondeinformatique.fr/actualites/lire-usa-et-ue-signent-un-accord-pour-succeder-au-privacy-shield-86255.html> consulté en ligne le 29 mars 2023.

⁸⁶⁸ CNIL, Déclaration 01/2022 du Comité européen de la protection des données sur l'annonce d'un accord de principe sur un nouveau cadre transatlantique pour la protection des données, 6 avril 2022.

⁸⁶⁹ Executive Order to Implement the European Union-U.S. Data Privacy Framework, 22 octobre 2022.

⁸⁷⁰ Parlement européen, « Le Parlement approuve le renforcement des pouvoirs d'Europol, mais pas sans contrôle », Communiqué de presse, 4 mai 2022.

administrations publiques des États membres, ou des personnes mandatées par le droit de l'Union pour le mettre en œuvre⁸⁷¹.

L'affaire « Cambridge Analytica » a, par exemple, amené le Parlement européen à créer une commission d'enquête de laquelle a résulté une résolution le 25 octobre 2018. En l'espèce, cette entreprise britannique s'est servie des données de 87 millions d'utilisateurs de Facebook pour établir des profils psychologiques d'utilisateurs et manipuler ainsi leurs opinions à des fins politiques grâce à de la publicité ciblée sur la plateforme Facebook⁸⁷².

Dans sa résolution, le Parlement demandait à la Commission « d'auditer les activités du secteur publicitaire sur les médias sociaux et de proposer une législation dans l'éventualité où le secteur et les parties concernées ne parviendraient pas à s'accorder sur un code de déontologie volontaire, avec des mesures dissuasives »⁸⁷³. Par ailleurs, il invitait les autorités en charge de la protection des données à caractère personnel « aux niveaux national et européen à mener une enquête approfondie sur Facebook et ses pratiques actuelles, de façon à ce que le nouveau mécanisme de contrôle de la cohérence du RGPD puisse servir de base à une réponse adaptée et efficace de l'Europe en matière de mesures répressives »⁸⁷⁴. Enfin, il demandait aux États membres de prendre des mesures « afin de pallier les risques pour la sécurité des réseaux et des systèmes d'information utilisés pour l'organisation des élections »⁸⁷⁵.

Le 26 janvier 2022, le Parlement européen avait demandé à plusieurs reprises la mise en place de principes éthiques guidant l'approche de l'Union européenne en matière de transformation numérique, ainsi que la garantie du plein respect des droits fondamentaux tels que la protection des données à caractère personnel, le droit à la vie privée, et la garantie du plein respect des principes tels que la neutralité technologique et du réseau, la protection des consommateurs, la fiabilité et l'inclusivité. La déclaration visait également à renforcer la protection des droits des utilisateurs, à soutenir les droits des travailleurs, à investir dans les

⁸⁷¹ TFUE, article 226. Cet article permet au Parlement de mettre en place des commissions d'enquête pour examiner les allégations des violations des droits de l'Union ou de mauvaise administration dans l'application du droit de l'Union européenne.

⁸⁷² Parlement européen, Résolution du Parlement européen du 25 octobre 2018 sur l'exploitation des données des utilisateurs de Facebook par Cambridge Analytica et les conséquences en matière de protection des données (2018/2855(RSP)), (2020/C 345/10), 25 octobre 2018.

⁸⁷³ Ibidem

⁸⁷⁴ Ibid.

⁸⁷⁵ Ibid.

compétences numériques, la santé mentale dans l'espace de travail numérique ainsi que le droit à la déconnexion⁸⁷⁶.

Sous-section 2 – La Cour de justice de l'Union européenne, garante du droit fondamental à la protection des données personnelles

Organe majeur dans l'architecture de la construction européenne dont les arrêts et avis marquent souvent le droit européen, la CJUE s'est notamment illustrée lorsqu'il a été question de la protection des données personnelles des passagers aériens.

§ 1 – La Cour de justice de l'Union européenne, un organe juridictionnel central dans la construction européenne

La CJUE est l'institution juridictionnelle de l'Union dont la principale mission consiste à assurer « le respect du droit dans l'interprétation et l'application des traités » comme l'affirme le premier alinéa de l'article 19 du TUE⁸⁷⁷, qui précise également que cet organe comprend la Cour de justice, le Tribunal et des tribunaux spécialisés.

L'influence du droit français a été décisive dans la création d'une juridiction européenne. En effet, la nécessité d'un contrôle de la légalité, comme le prévoit le droit administratif français⁸⁷⁸, a amené les initiateurs de la construction européenne à mettre en place, au sein de la Communauté économique du charbon et de l'acier, d'une Cour de justice statuant comme un juge interne de la Communauté⁸⁷⁹.

Le Traité instituant la Communauté européenne du charbon et de l'acier (CECA), signé à Paris le 18 avril 1951, a institué une Cour de justice, dans son article 7⁸⁸⁰. Les articles 33 et 44 organisaient les compétences de cette juridiction⁸⁸¹. Outre les compétences similaires à celles du contentieux administratif français, ce traité a attribué à la Cour, une compétence de pleine juridiction à l'égard des manquements des États membres (à l'article 88), ainsi qu'une compétence d'avis en cas de révision du Traité (à l'article 95, alinéa 4)⁸⁸².

La Cour de justice actuelle est composée d'un juge par État membre et est assistée d'avocats généraux. Ces juges et les avocats généraux sont nommés d'un commun accord par les États

⁸⁷⁶ Parlement européen, « Les institutions européennes approuvent la déclaration sur les droits et principes numériques », Communiqué de presse, 15 décembre 2022.

⁸⁷⁷ TUE, article 19, alinéa 1.

⁸⁷⁸ A. DELBLOND, *Droit administratif*, Larcier, Collection Manuels Larcier, 2009.

⁸⁷⁹ V. M. LAGRANGE, « La Cour de justice des Communautés européennes : du plan Schuman à l'Union européenne », *Revue trimestrielle de droit européen*, Dalloz, 1978.

⁸⁸⁰ Traité instituant la Communauté européenne du Charbon et de l'Acier, 18 avril 1951, Paris.

⁸⁸¹ Ibidem

⁸⁸² Ibid.

membres. Les candidats à ces fonctions doivent faire montre de toutes les garanties d'indépendance.

Concrètement, ces derniers doivent soit réunir les conditions requises pour exercer les plus hautes fonctions juridictionnelles dans leurs pays respectifs, soit être des juristes possédant des compétences notoires⁸⁸³. Un comité spécial est créé, chargé de donner son avis sur les candidatures, et composé lui-même de sept experts juridiques qui sont soit d'anciens membres de la Cour de justice et du Tribunal ou des membres des juridictions nationales suprêmes, soit des juristes possédant des compétences reconnues. Les membres de la Cour sont nommés pour une durée de six ans renouvelable⁸⁸⁴. La Cour est renouvelée par moitié tous les trois ans. Enfin, avant d'entrer en fonction, les juges doivent prêter serment d'exercer leurs fonctions, en pleine impartialité, et en toute conscience et de ne rien divulguer du secret des délibérations.

Les juges sont appelés à désigner, parmi eux, le président et le vice-président de la Cour de justice⁸⁸⁵. La durée de leur mandat est de trois ans, renouvelable. Le président représente la Cour et doit diriger ses travaux. Ce dernier est assisté par un vice-président qui le remplace en cas d'empêchement. En principe, la Cour est divisée en chambres de trois et de cinq juges. Toutefois, dans des cas particuliers, elle peut siéger en grande chambre, de quinze juges, ou en assemblée plénière. Enfin, la Cour nomme un greffier pour une période de six ans, renouvelable. Ce greffier est notamment chargé d'assister les membres de la Cour dans tous les actes de leur ministère.

La Cour est compétente dans le cadre des recours en manquement, en annulation et en carence introduits, soit par un État membre contre le Parlement européen et/ou contre le Conseil, sauf pour les actes de ce dernier en matière d'aides d'État, de dumping et de compétences d'exécution, soit par une institution de l'Union contre une autre institution. La Cour est également compétente pour statuer à titre préjudiciel sur l'interprétation du droit européen et sur la validité des actes adoptés par les institutions, organes ou organismes de l'Union. Enfin, la Cour peut être saisie de pourvois, limités aux questions de droit, et contre les arrêts et ordonnances du Tribunal⁸⁸⁶.

⁸⁸³ Cour de justice de l'Union européenne, *Fiche d'orientation*, Dalloz.

⁸⁸⁴ Ibidem

⁸⁸⁵ Ibid.

⁸⁸⁶ Ibid.

§ 2 – La Cour de justice de l'Union européenne, un organe juridictionnel décisif dans la mise en avant de la protection des données personnelles des passagers aériens

La Cour européenne des droits de l'homme a affirmé le droit à la protection de la vie privée comme un droit fondamental, en exigeant l'établissement de « règles claires et détaillées » pour le traitement des données et des « garanties suffisantes contre les risques d'abus et d'arbitraire »⁸⁸⁷. Cette approche pionnière dans la protection des données personnelles, qui inclut toute information relative à une personne identifiée ou identifiable⁸⁸⁸, a servi de modèle pour la Cour de justice de l'Union européenne. Les juges de cette cour ont souligné la nécessité d'un « contrôle rigoureux » sur ces traitements⁸⁸⁹. Toutefois, la marge de manœuvre des États membres dans l'application de ces principes varie en fonction de la sensibilité des données et des objectifs poursuivis⁸⁹⁰, pouvant être étroite dans certains cas ou, plus rarement⁸⁹¹, plus large.

C'est dans le sillage de la jurisprudence strasbourgeoise que la Cour de Justice a construit sa jurisprudence protectrice des droits fondamentaux, notamment en matière de vie privée et de données personnelles⁸⁹². Elle a garanti cette protection à travers, dans un premier temps, les principes généraux du droit, puis, à la suite de l'entrée en vigueur du Traité de Lisbonne, à l'appui des droits fondamentaux consacrés en droit européen, respectivement le droit au respect de la vie privée et le droit à la protection des données à caractère personnel prévus aux articles 7 et 8 de la Charte. En outre, cette protection des données personnelles s'inscrit dans le cadre de la construction européenne qui soutient la libre circulation. En effet, le fait d'assurer un niveau de protection élevé et uniforme est censé permettre d'éviter des entraves à la liberté de circulation au sein du marché intérieur⁸⁹³.

La Cour a précisé la nature de son contrôle au regard de la Charte dans l'arrêt *Volker Schecke GbR und Markus et a.*⁸⁹⁴, dans lequel elle a affirmé que les limitations apportées au droit à la

⁸⁸⁷ CJUE, *Klass et autres c/ Allemagne*, arrêt du 6 septembre 1978, requête n° 5029/71, § 55-56. *Rotaru c/ Roumanie*, arrêt du 4 mai 2000, requête n° 28341/95, § 43. *S. et Marper c. Royaume-Uni*, arrêt du 4 décembre 2008, requêtes n° 30562/04 et 30566/04, § 104-105.

⁸⁸⁸ H. SURREL, « La protection des données à caractère personnel, domaine emblématique des interactions jurisprudentielles entre cours européennes et Conseil constitutionnel », Titre VII, 2019/1, 2019, en ligne à URL : https://www.cairn.info/article.php?ID_ARTICLE=TVII_002_0051 consulté en ligne le 29 mars 2023.

⁸⁸⁹ Cour européenne des droits de l'Homme, *Leander c/Suède*, § 48, 26 mars 1987.

⁸⁹⁰ H. SURREL, op. cit.

⁸⁹¹ Cour européenne des droits de l'Homme, Gr. Ch., 4 déc. 2008, *S. et Marper c/Royaume-Uni*, §§ 99, 102, 104, empreintes digitales, profils ADN et échantillons cellulaires ; déc., 11 janv. 2018, n° 38334/08, *Anchev c/Bulgarie*, informations sur les personnes ayant collaboré avec les anciens services de sécurité.

⁸⁹² H. SURREL, op. cit.

⁸⁹³ Ibidem

⁸⁹⁴ CJUE, *Volker und Markus Schecke GbR (C-92/09) et Hartmut Eifert (C-93/09) c/ Land Hessen*, (pt 52), 9 novembre 2010.

protection des données à caractère personnel « correspondent à celles tolérées dans le cadre de l'article 8 de la CEDH ». Par ailleurs, la Cour n'a pas manqué de rappeler le caractère strict de son contrôle qui s'accompagne d'une marge d'appréciation réduite du législateur de l'Union, comme dans l'affaire *Digital Rights Ireland Ltd.*

En se référant à la jurisprudence européenne, en particulier à l'arrêt *S. et Marper*⁸⁹⁵, le juge européen a examiné, à la lumière du droit au respect de la vie privée et du droit à la protection des données personnelles, l'existence de garanties adéquates contre les risques d'abus liés à la conservation des données relatives aux communications électroniques. Ces données, lorsqu'elles sont considérées dans leur ensemble, peuvent en effet permettre de tirer des conclusions très précises sur la vie privée des individus⁸⁹⁶.

En lien avec la jurisprudence récente de la CJUE sur la protection des données à caractère personnel, il est manifeste que « la Charte des droits fondamentaux n'est pas un tigre de papier »⁸⁹⁷. En effet, dans un arrêt du 21 juin 2022 concernant le traitement des données personnelles des passagers aériens, la Cour a affirmé que, en l'absence d'une menace terroriste réelle, actuelle ou prévisible, le droit européen interdit une législation nationale qui autoriserait le transfert et le traitement des données PNR pour les vols intra-UE ainsi que pour les autres moyens de transport au sein de l'Union⁸⁹⁸.

Selon la Cour, la directive européenne sur le PNR comporte des ingérences graves aux droits à la vie privée et à la protection des données à caractère personnel, protégés par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, et celles-ci doivent être strictement limitées compte tenu de l'importance de l'objectif d'intérêt général poursuivi⁸⁹⁹. C'est pourquoi, le transfert, le traitement et la conservation des données PNR prévus par la directive peuvent être considérés comme étant limités au strict nécessaire aux fins de la lutte contre les infractions terroristes et les formes graves de criminalité, à la condition que les pouvoirs prévus par la directive fassent l'objet d'une interprétation restrictive⁹⁰⁰.

La Cour a considéré que le système établi par la directive PNR ne doit couvrir que les informations clairement identifiables et circonscrites dans les rubriques figurant dans l'annexe

⁸⁹⁵ CJUE, *S. et Marper c/ Royaume-Uni*, arrêt du 4 décembre 2008, requêtes n° 30562/04 et 30566/04, § 104-105.

⁸⁹⁶ CJUE, Gr. Ch., aff. C-293/12 et C-594/12, pt 27, 8 avr. 2014.

⁸⁹⁷ Voir : M.-C. DE MONTECLER, Dalloz, *L'actualité juridique droit administratif*, AJDA, 2014.

⁸⁹⁸ CJUE, 21 juin 2022, aff. C-817/19.

⁸⁹⁹ Ibidem

⁹⁰⁰ Ibid.

I de celle-ci, lesquelles sont en rapport avec le vol effectué et avec le passager concerné⁹⁰¹. Par ailleurs, elle précisa que l'application de ce système doit être limitée aux infractions terroristes et aux seules formes graves de criminalité présentant un lien objectif, à tout le moins indirect, avec le transport aérien des passagers⁹⁰². Elle ajouta que l'éventuelle extension de l'application de la directive, à tout ou partie des vols intra-UE, doit être limitée au strict nécessaire. En outre, s'agissant en particulier du délai de conservation des données PNR, les juges européens s'opposent à une législation nationale qui prévoit une durée générale de conservation de ces données de cinq ans, applicable indifféremment à tous les passagers aériens⁹⁰³.

Les juges de Luxembourg se sont déjà prononcés sur la validité de textes dont l'objet est le transfert des données à caractère personnel sur la base du respect des droits fondamentaux, notamment du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, garantis respectivement par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. En 2017, la Cour de justice avait conclu que « l'accord PNR ne peut pas être conclu sous sa forme actuelle en raison de l'incompatibilité de plusieurs de ses dispositions avec les droits fondamentaux reconnus par l'Union »⁹⁰⁴ bien qu'elle ait admis que le transfert, la conservation et l'utilisation systématique des données de dossiers passagers que prévoit l'accord sont, pour l'essentiel admissibles.

En l'espèce, le juge européen a admis des ingérences dans les droits fondamentaux des passagers aériens européens au motif qu'elles visaient la réalisation d'un objectif de sécurité publique contre les actes terroristes et les crimes transnationaux. Cependant, le problème résidait dans plusieurs dispositions de l'accord qui n'étaient pas limitées au strict nécessaire et ne prévoyaient pas des règles claires et précises. Le transfert des données sensibles vers le Canada devait être justifié par d'autres motifs que ceux visant la protection de la sécurité publique. À défaut, ces dispositions étaient jugées incompatibles avec le respect des droits fondamentaux du fait d'un risque de traitement contraire au principe de non-discrimination.

En juillet 2017, les juges de Luxembourg se sont prononcés pour la première fois sur la comptabilité d'un accord international au regard de la Charte des droits fondamentaux de l'Union, en déclarant donc incompatibles avec les articles 7 et 8 de celle-ci, les dispositions du projet d'accord sur le transfert des données des dossiers passagers signé, en 2014, entre

⁹⁰¹ Ibid.

⁹⁰² Ibid.

⁹⁰³ Ibid.

⁹⁰⁴ Avis 1/15, CJUE 26 juillet 2017.

l'Union européenne et le Canada⁹⁰⁵. Cette jurisprudence marque la préoccupation de la Cour pour atteindre un équilibre entre liberté individuelle et sécurité collective. En effet, l'arrêt *Digital Rights Ireland Ltd (C-293/12)* du 8 avril 2014, précédemment commenté, a annulé dans son intégralité et *ab initio* la directive « rétention des données de communications électroniques ». Le juge européen a ici clairement censuré le stockage de masse de données et imposé un certain nombre de garde-fous qui s'appliquent dans le cadre de la directive PNR⁹⁰⁶.

Avant ces arrêts rendus après le Traité de Lisbonne, la Cour de justice, saisie par les eurodéputés, avait décidé, le 30 mai 2006, d'annuler l'accord de Washington sur le PNR du 28 mai 2004 au motif que la décision d'adéquation prise par la Commission ne relevait pas du champ d'application de la directive 95/46 sur laquelle elle l'avait fondée. Le juge européen avait estimé que l'article 95 du traité CE ne constituait pas une base juridique appropriée pour le transfert des données PNR, qui « sont essentiellement utilisées pour assurer la sécurité publique et dans le cadre des activités des autorités publiques dans les domaines relevant du droit pénal »⁹⁰⁷.

Ces positions de la Cour de justice confirment son rôle d'organe juridictionnel décisif dans la mise en avant de la protection des données personnelles des passagers aériens au sein de l'Union européenne⁹⁰⁸. Cette jurisprudence vise à ce que l'arsenal juridique mis en place par les États sur l'utilisation des données PNR pour la prévention, la détection, l'investigation et la poursuite des infractions terroristes ainsi que de la criminalité transnationale grave respecte les exigences juridiques de la Charte des droits fondamentaux, tout en fournissant un nouvel outil efficace de lutte contre ces infractions dans un contexte politique où la recrudescence des attentats terroristes appellent un renforcement de l'arsenal répressif.

Sous-section 3 – Le Comité européen de la protection des données, le garant d'un nouvel ordre

Organe européen indépendant contribuant à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne, le Comité européen de la protection des données n'a cessé d'encourager la coopération entre les autorités de l'Union européenne pour assurer une meilleure protection des données personnelles des passagers aériens.

⁹⁰⁵ E. AUTIER, « La CJUE déclare incompatible l'accord des données PNR signé avec le Canada », *Dalloz*, 28 juillet 2017.

⁹⁰⁶ S. PEYROU, « Le PNR européen à la croisée des chemins : protection des données et lutte contre le terrorisme », *GDR-ELSJ*, 25 janvier 2015.

⁹⁰⁷ Commission européenne, « Communiqué de presse », 19 juin 2006

⁹⁰⁸ B. STIRN, « Europe et droits fondamentaux », *Le Grand Continent*, 6 novembre, 2019, en ligne à URL : <https://legrandcontinent.eu/fr/2019/11/06/europe-et-droits-fondamentaux/> consulté le 13 novembre 2023.

§ 1 – La substitution du Groupe 29 par le Comité européen de la protection des données

La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après la « directive ») confiait déjà à un groupe de travail, reconnu comme le « Groupe 29 », la mission principale d'aider à la mise en œuvre de la directive en soutenant son application uniforme dans les États membres⁹⁰⁹.

Constitué des autorités de protection des données européennes des États membres et de la Commission, le Groupe 29 avait pour missions d'examiner la mise en œuvre homogène de la directive, de donner un avis à la Commission sur le niveau de protection dans l'Union et dans les pays tiers, de conseiller la Commission sur tout projet de modification de la directive ainsi que sur tout autre projet de mesures de l'Union ayant une incidence sur la protection des données à caractère personnel, ou enfin de délivrer un avis sur les codes de conduite élaborés au niveau européen⁹¹⁰.

Ce groupe pouvait également « émettre de sa propre initiative des recommandations sur toute question concernant la protection des personnes à l'égard du traitement de données à caractère personnel dans la Communauté »⁹¹¹. De façon régulière, et tout au long de son existence, de sa propre initiative ou après consultation, le Groupe 29 a émis divers avis et recommandations⁹¹². Cette activité en faisait une figure hybride entre « super-régulateur » au niveau européen et groupe de coopération des autorités nationales.

En 2010, la Commission a communiqué une « approche globale de la protection des données à caractère personnel dans l'Union européenne »⁹¹³ selon laquelle elle aspirait à renforcer le cadre institutionnel européen afin de mieux garantir le respect des règles de protection des données personnelles. Cette communication a examiné les moyens de renforcer le statut et les pouvoirs des autorités nationales de protection des données dans un cadre juridique nouveau, d'améliorer la coopération entre les autorités de protection des données à caractère personnel et de garantir une mise en œuvre plus cohérente des règles européennes en matière de

⁹⁰⁹ Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Considérant 65.

⁹¹⁰ Article 30 de la directive.

⁹¹¹ Article 30, § 3 de la directive.

⁹¹² R. ROBERT, « Le Comité européen de la protection des données : le garant d'un nouvel ordre ? », *Le règlement général sur la protection des données*, Dalloz, 2018.

⁹¹³ Commission européenne, « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », 4 novembre 2010, COM(2010), 609 final, p. 20, en ligne à URL : https://edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_fr consulté en ligne le 29 mars 2023.

protection des données dans tout le marché intérieur, notamment en renforçant le rôle des contrôleurs nationaux⁹¹⁴.

La réforme du cadre européen de protection des données personnelles a été une occasion pour le législateur européen de créer le Comité européen de la protection des données personnelles⁹¹⁵, en remplacement du Groupe 29, afin d'assurer une meilleure application uniforme et cohérente du Règlement général sur la protection des données dans l'Union européenne (ci-après RGPD). L'une des missions de ce nouvel organe européen est d'intervenir dans le mécanisme de contrôle de la cohérence qui, avec et au-delà du mécanisme de guichet unique, devrait permettre une application harmonieuse des règles européennes en matière de protection des données personnelles.

§ 2 – Le Comité européen de la protection des données, un acteur indépendant en charge de la protection des données personnelles des citoyens européens

L'article 68 § 1^{er} du RGPD donne au Comité une personnalité juridique et en fait un organe de l'Union⁹¹⁶, ce qui n'était pas le cas du Groupe 29 qui avait le statut de groupe d'experts. L'attribution de ce statut a été jugé nécessaire par l'Union afin de permettre à ce nouvel organe d'atteindre ses objectifs.

Le Comité se compose du chef d'une autorité de contrôle de chaque État membre et du Contrôleur européen de la protection des données ou de leurs représentants respectifs comme le rappelle le second paragraphe de l'article 68 du RGPD. La Commission a le droit de participer aux activités et aux réunions du Comité mais n'a pas de droit de vote⁹¹⁷. Le Comité exerce les missions et les pouvoirs qui lui sont conférés en toute indépendance et ne reçoit aucune instruction de quiconque dans l'exercice de ces derniers⁹¹⁸.

Afin de pouvoir appliquer de manière cohérente le règlement européen, le Comité assume 25 missions, parmi lesquelles : surveiller et garantir la bonne application du règlement ; conseiller la Commission ; publier des lignes directrices, recommandations et bonnes pratiques ; faire le bilan de leur bonne application ; encourager l'élaboration de codes de conduite et la mise en place de mécanismes de certification et de labels ; rendre des avis à la

⁹¹⁴ Ibidem.

⁹¹⁵ R. ROBERT, « Le Comité européen de la protection des données : le garant d'un nouvel ordre ? », *Le règlement général sur la protection des données*, Dalloz, 2018.

⁹¹⁶ Article 68, §1 RGPD.

⁹¹⁷ Article 68, §5 RGPD.

⁹¹⁸ Article 69, § 1 et 2 RGPD.

Commission et sur les projets de décision des autorités nationales de contrôle chefs de file ainsi que sur les codes de conduite émis au niveau de l'Union⁹¹⁹.

Par ailleurs, le Comité est appelé à rédiger un rapport annuel sur la protection des personnes physiques à l'égard du traitement de leurs données dans l'Union, rendu public et communiqué au Parlement européen, au Conseil et à la Commission. Cette communication a pour but de présenter le bilan de l'application pratique des recommandations, lignes directrices et bonnes pratiques⁹²⁰. À la demande du Comité, ses débats peuvent être tenus confidentiels⁹²¹.

Le Comité prend ses décisions à la majorité simple de ses membres, sauf disposition contrairement du règlement⁹²². Il adopte son règlement intérieur à la majorité de deux tiers de ses membres. Il détermine ses modalités de fonctionnement. Les règles d'élections du Président du Comité sont posées par l'article 73 du RGPD⁹²³ : le Comité élit en son sein, à la majorité simple, son président et deux vice-présidents. Ces derniers sont élus pour un mandat de cinq ans, renouvelable une fois. Les missions du président sont prévues à l'article 74⁹²⁴ dont celles de convoquer les réunions du Comité et d'établir l'ordre du jour, de notifier les décisions adoptées par le Comité, de veiller à l'accomplissement, dans les délais, des missions du Comité. Le Comité fixe dans son règlement intérieur la répartition des tâches entre le président et les vice-présidents.

L'article 75 prévoit un secrétariat pour le Comité assuré par le Contrôleur européen de la protection des données chargé de faire respecter, auprès des institutions de l'Union européenne, les dispositions relatives à la protection des données, en application du règlement du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données⁹²⁵. Les missions du secrétariat sont accomplies sous l'autorité exclusive du président du Comité.

Il est à noter que le personnel du Contrôleur européen de la protection des données qui participe à l'exercice des tâches que le règlement confie au Comité est soumis à une structure

⁹¹⁹ Article 70, RGPD.

⁹²⁰ Article 71, RGPD.

⁹²¹ Article 76, RGPD.

⁹²² Article 72, RGPD.

⁹²³ Article 73, RGPD.

⁹²⁴ Article 74, RGPD.

⁹²⁵ Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

hiérarchique distincte de celle du personnel qui participe à l'exercice des tâches confiées au Contrôleur européen de la protection des données⁹²⁶.

Ce secrétariat est chargé des missions suivantes : la gestion courante du Comité ; la communication entre les membres du Comité, son président et la Commission ; la communication avec le public et les autres institutions ; l'utilisation des voies électroniques pour la communication interne et externe ; la préparation et le suivi des réunions du Comité ; la traduction des informations utiles ; la préparation, la rédaction et la publication d'avis, de décisions relatives au règlement des litiges entre autorités de contrôle et d'autres textes adoptés par le Comité⁹²⁷.

Récemment, le 28 février 2023⁹²⁸, le Comité a adopté un avis sur le projet de décision d'adéquation entre Européens et Américains dans lequel il se félicitait d'améliorations substantielles dont l'adoption par les États-Unis d'exigences qui reprennent, d'une part, les principes de nécessité et de proportionnalité dans la collecte des données à caractère personnel et, d'autre part, le nouveau mécanisme de recours pour les personnes concernées de l'Union européenne. En effet, le président américain a adopté, le 7 octobre 2022, un nouveau cadre juridique – l'Executive Order 14086⁹²⁹ – dans le but de renforcer les garanties visant la collecte et l'utilisation des données à caractère personnel par les services de renseignement américains⁹³⁰.

Ce nouveau projet a été soumis à la Commission européenne afin que celle-ci évalue si le cadre juridique permet d'assurer un niveau de protection adéquat des données à caractère personnel des Européens⁹³¹. La Commission a soumis un projet de décision pour avis au Comité avant d'adopter définitivement sa décision reconnaissant le caractère adéquat de ce nouveau dispositif. C'est dans ce contexte que le Comité a adopté et publié son avis sur le projet de décision d'adéquation⁹³².

⁹²⁶ « La création du Comité européen de la protection des données en remplacement du 'G29' », *Répertoire de droit européen*, Dalloz, 2022.

⁹²⁷ Ibidem

⁹²⁸ Avis 5/2023 relatif au projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE-États-Unis, 23 février 2023.

⁹²⁹ Executive Order 14086 Enhancing Safeguards for United States Signals Intelligence, 7 octobre 2022.

⁹³⁰ EDPB, "EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain", News, EDPB, 28 February 2023 en ligne à URL : https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_fr consulté en ligne le 2 mars 2023.

⁹³¹ Agence des droits fondamentaux de l'Union européenne, *Manuel de droit européen en matière de protection des données*, éditions 2018, avril 2018.

⁹³² Ibidem.

Tout en relevant les améliorations apportées par les représentants américains, le Comité a exprimé des préoccupations et a demandé aux parties des éclaircissements sur plusieurs points, qui concernent notamment les droits des personnes concernées, les transferts ultérieurs, la portée des exemptions, la collecte temporaire massive de données et le fonctionnement pratique du mécanisme de recours⁹³³.

Le Comité a estimé qu'il accueillerait favorablement l'adoption et l'entrée en vigueur de la décision d'adéquation, sous réserve qu'elle soit conditionnée à l'adoption de politiques et de procédures actualisées pour mettre en œuvre l'Executive Order 14086⁹³⁴ par toutes les agences de renseignement américaines. Ce document a mis en place, d'une part, des limitations et des garanties pour toutes les activités de renseignement indépendamment du lieu où elles se déroulent, et organisé, d'autre part, un nouveau mécanisme de recours par lequel ces garanties peuvent être invoquées par des particuliers. Le Comité avait recommandé à la Commission d'évaluer ces politiques et procédures mises à jour et de partager son évaluation avec celui-ci.

Le projet de décision d'adéquation publié par la Commission européenne⁹³⁵ le 13 décembre 2022 est fondé sur le U.S. Data Privacy Framework (DPF), un cadre réglementaire relatif aux transferts de données personnelles entre l'Europe et les États-Unis, destiné à remplacer le Privacy Shield invalidé par la CJUE dans l'arrêt Schrems II. Le DPF pose les principes du cadre de confidentialité des données UE-États-Unis qui ont été publiés par le département américain du commerce. Le DPF ne s'applique qu'aux organisations américaines qui se sont auto-certifiées. Le Comité a ainsi adopté son avis sur le projet de décision qui tient compte à la fois des aspects commerciaux mais également de l'accès et de l'utilisation des données par les autorités publiques américaines⁹³⁶.

En ce qui concerne les aspects commerciaux, le Comité avait loué un certain nombre de mises à jour apportées aux principes du DPF en notant par ailleurs qu'un certain nombre de principes restaient cependant essentiellement les mêmes que ceux établis dans le cadre du Privacy Shield⁹³⁷. À ce titre, certaines inquiétudes ont subsisté, par exemple, concernant

⁹³³ EDPB, "EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain", News, EDPB, 28 February 2023 en ligne à URL : https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_fr consulté en ligne le 2 mars 2023.

⁹³⁴ Executive Order 14086, op. cit.

⁹³⁵ Commission européenne, Décision d'adéquation relative au Cadre de Protection de la Vie Privée UE-États-Unis, 13 décembre 2022.

⁹³⁶ EDPB, "EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain", News, EDPB, 28 February 2023 en ligne à URL : https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_fr consulté en ligne le 2 mars 2023.

⁹³⁷ Comité Européen de la Protection des Données, Avis sur le projet de décision d'adéquation pour le Cadre de Protection de la Vie Privée UE-États-Unis, 13 décembre 2022.

certaines dérogations au droit d'accès, l'absence de définitions clés, le manque de clarté quant à l'application des principes DPF aux sous-traitants, la large dérogation au droit d'accès pour les informations publiques disponibles et l'absence de règles spécifiques sur la prise de décision automatisée et le profilage. Le Comité a fait valoir, en outre, que le niveau de protection ne devait pas être compromis par des transferts ultérieurs, c'est pourquoi il invita la Commission à préciser que les garanties imposées par le destinataire initial à l'importateur dans le pays tiers doivent être effectives à la lumière de la législation du pays tiers avant un transfert ultérieur⁹³⁸.

En outre, le Comité a demandé à la Commission de clarifier la portée des exemptions concernant l'obligation d'adhérer aux principes du DPF et souligné l'importance d'une surveillance ainsi que d'une application efficace du DPF. Ces aspects sont étroitement surveillés par le Comité et doit assurer l'efficacité des voies de recours fournies aux personnes concernées résidentes de l'Union européenne dont les données sont traitées en violation du DPF.

En ce qui concerne l'accès du gouvernement aux données transférées aux États-Unis, le Comité a reconnu les améliorations significatives apportées par le décret exécutif américain, l'Executive Order 14086⁹³⁹. En effet, ce dernier a introduit les concepts de nécessité et de proportionnalité en ce qui concerne la collecte de données par les autorités de renseignement américaines⁹⁴⁰.

Par ailleurs, le nouveau mécanisme de recours, qui crée des droits pour les citoyens européens, est soumis à l'examen du Conseil de surveillance, Privacy and Civil Liberties Oversight Board (PCLOB)⁹⁴¹. Le décret américain a également consacré davantage de garanties pour assurer l'indépendance de la Data Protection Review Court (DPRC)⁹⁴², en comparaison du mécanisme précédent du médiateur, et prévu des pouvoirs plus efficaces pour remédier aux violations, y compris des garanties supplémentaires pour les personnes concernées. Le CEPD a aussi souligné qu'un suivi étroit est nécessaire concernant

⁹³⁸ CEPD, Avis 5/2023 relatif au projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE-États-Unis, 28 février 2023.

⁹³⁹ Executive Order 14086, Op. cit.

⁹⁴⁰ Comité Européen de la Protection des Données, Avis sur le projet de décision d'adéquation pour le Cadre de Protection de la Vie Privée UE-États-Unis, 13 décembre 2022.

⁹⁴¹ Le décret américain (EU-US Data Privacy Framework) charge également le Conseil de surveillance de la protection de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board - PCLOB) d'examiner les mises à jour politiques des services de renseignement pour tenir compte de la vie privée et des libertés civiles des personnes et de procéder à un examen annuel.

⁹⁴² The Data Protection Review Court est une autorité de régulation américaine dont l'objet est de statuer sur les demandes et ordonner des mesures correctives si nécessaire en faveur des citoyens européens.

l'application pratique des principes de nécessité et de proportionnalité nouvellement introduits. Une plus grande clarté est également nécessaire en ce qui concerne la collecte en masse temporaire et la conservation ainsi que la diffusion ultérieures des données collectées en masse.

Le Comité s'était également montré préoccupé par l'absence d'obligation d'autorisation préalable par une autorité indépendante pour la collecte de données massive prévue dans le cadre de l'Executive Order 12333 du 4 décembre 1981 ainsi que par l'absence de contrôle indépendant systématique *ex post* par un tribunal ou un organisme indépendant équivalent. En ce qui concerne l'autorisation préalable de surveillance rendue de manière indépendante par la Foreign Intelligence Surveillance Act (FISA), au titre de la section 702⁹⁴³, le PCLOB a regretté que la juridiction de FISA ne contrôle pas la conformité avec l'Executive Order 14086 lorsqu'elle certifie des programmes autorisant le profilage de personnes non-américaines alors même que les autorités de renseignement qui exécutent le programme sont liées par celui-ci.

Le Comité a par ailleurs considéré que des rapports rendus par le PCLOB sur la mise en œuvre des garanties de l'Executive Order 14086 et sur la manière dont ces garanties sont appliquées lorsque des données sont collectées en vertu de la section 702 de la FISA et de l'Executive Order 12333 seront particulièrement utiles dans l'avenir. En ce qui concerne le mécanisme de recours, le Comité a reconnu les garanties supplémentaires intégrées telles que le rôle des avocats spéciaux et l'examen du mécanisme de recours par le PCLOB⁹⁴⁴.

Toutefois, le Comité a continué d'exprimer sa préoccupation sur la mise en œuvre d'une réponse standard du DPRC pour notifier au plaignant soit qu'aucune violation couverte n'a été identifiée, soit, au contraire, qu'une remédiation appropriée a été émise à la suite de l'identification d'une violation. Il s'agit d'un sujet d'autant plus préoccupant pour le Comité que cette décision ne peut pas faire l'objet d'un appel. Conséquemment, le Comité a invité la Commission à surveiller de près le fonctionnement pratique de ce mécanisme⁹⁴⁵.

⁹⁴³ Législation du Congrès des États-Unis de 1978 décrivant les procédures des surveillances physiques et électronique, ainsi que la collecte d'information sur des puissances étrangères soit directement, soit par l'échange d'informations avec d'autres puissances étrangères.

⁹⁴⁴ EDPB, "EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain", News, EDPB, 28 February 2023 en ligne à URL : https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_fr consulté en ligne le 2 mars 2023

⁹⁴⁵ Ibidem

§ 3 – Le Comité européen de la protection des données, un acteur investi dans la protection des données personnelles des passagers aériens

C'est dans le cadre de l'espace de liberté, de sécurité et de justice que le Groupe 29, devenu Comité européen de la protection des données, a émis des avis sur les données des dossiers passagers aériens ainsi que sur le modèle européen en matière d'échange d'informations, Europol ainsi que la stratégie de l'Union en matière de cybersécurité et les frontières intelligentes⁹⁴⁶.

Le Groupe 29 a ainsi émis un avis lors la conclusion de l'accord euro-américain de 2004, qui a soulevé de vives inquiétudes et un concert de résistances. Ces résistances allaient de mises en garde aux protestations les plus fermes. Sur la question des exigences imposées en la matière, dans cet avis rendu le 24 octobre 2002, le Groupe 29 s'est alarmé au regard de la protection des données personnelles des citoyens européens⁹⁴⁷. Selon ce dernier, le système de transmission des données passagers couvrait des catégories trop étendues des données personnelles. Une telle transmission équivalait à la mise en place d'une surveillance généralisée des citoyens européens par un État tiers. De ce fait, elle constituait un outil dont l'objectif était de permettre l'élaboration d'une base de données d'individus susceptibles d'être profilés.

Les experts européens ont considéré que bien qu'il n'existât pas de disposition conférant une compétence à la Communauté en matière de protection des données personnelles, la Commission a invoqué les articles 95 et 300 du Traité instituant la Communauté européenne pour conclure cet accord⁹⁴⁸. Or, le groupe rappela que l'article 95 de ce traité concerne l'établissement et le fonctionnement du marché intérieur et qu'il ne confère pas une compétence externe à la Communauté pour négocier ou pour signer des accords internationaux avec des pays tiers en matière de transfert de données personnelles. Ce même groupe a ensuite adopté deux autres avis⁹⁴⁹ prenant en compte l'évolution enregistrée au cours

⁹⁴⁶ Commission, « Dix-septième rapport du groupe de travail "Article 29" sur la protection des données », 2013.

⁹⁴⁷ Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis (11647/02/FR/Final).

⁹⁴⁸ S. CLAVET, « Les conséquences de l'accord Passenger Name Record sur la protection des droits fondamentaux en Europe », *Droits fondamentaux*, n° 8, janvier 2010 - décembre 2010.

⁹⁴⁹ Avis 4/2003, du 13 juin 2003, sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers (11070/03/FR ; Avis 2/2004, du 29 janvier 2004, sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (US CBP) (10019/04/FR), disponibles via le site de la Commission.

des négociations entre Européens et Américains, les premiers projets d'accord entre les deux parties ne l'ayant pas convaincu⁹⁵⁰.

Puis, dans le cadre de la proposition de directive européenne sur les dossiers passagers, le Groupe 29, dans un avis 10/2011 adopté le 5 avril 2011⁹⁵¹, a mis en doute la nécessité et la proportionnalité des systèmes PNR. Pour lui, ni la nécessité de la mesure ni sa proportionnalité aux objectifs poursuivis n'étaient pertinemment justifiées malgré les efforts réalisés pour mieux encadrer le dispositif par rapport à la proposition de décision-cadre de 2007. Il s'agit d'une position qu'il a maintenu à l'égard de la proposition de 2011. Le groupe a considéré que les finalités de la directive n'étaient pas suffisamment précises, la durée de conservation excessive, les droits des personnes concernées insuffisants, la liste des données transmises trop large et les possibilités de transfert ultérieur à des États tiers trop étendues.

Dans une lettre du 9 octobre 2013, le groupe s'est également prononcé concernant la proposition de décision du Conseil relative à la conclusion de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement des données des dossiers passagers⁹⁵². Le groupe de travail avait considéré que la minimisation des données est de première importance pour la vie privée des passagers. Il avait donc recommandé que la nécessité de chaque élément figurant dans la liste de données soit examinée de manière distincte, du côté canadien.

Le groupe de travail avait conseillé de réexaminer les définitions des termes tels que prévention, détection, investigation et poursuites des infractions terroristes ou des formes graves de criminalité transnationale, à l'époque considérés comme trop vagues. Le groupe de travail avait, par ailleurs, regretté que l'accord permette le traitement de données sensibles par les autorités canadiennes et avait recommandé, dans le cas de violations de données ou

⁹⁵⁰ Avis 5/2007 concernant le nouvel accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure conclu en juillet 2007 (01646/07/EN, WP 138) et Avis 4/2003 sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers (11070/03/EN, WP 78) ; Avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers (622/10/EN, WP 178) ; Avis 10/2011 du groupe de travail «Article 29» sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers 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 (00664/11/EN, WP 181) ; Avis 01/2014 du Groupe de travail « sur l'article 29 » sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif du 27 février 2014 (536/14/FR, WP 211).

⁹⁵¹ Avis 10/2011 du groupe de travail «Article 29» sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers 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 (00664/11/EN, WP 181).

⁹⁵² Commission, « Dix-septième rapport du groupe de travail "Article 29" sur la protection des données », 2013.

d'incidents liés à la protection des données, que les autorités européennes chargées de la protection des données concernées soient informées.

Concernant le contrôle de la mise en œuvre de l'accord, le groupe avait suggéré et recommandé que les parties demandent aux transporteurs aériens de fournir aux passagers des informations sur les raisons, l'objectif, l'utilisation, le droit d'accès, le droit à l'information, les droits de correction et de recours relatifs au traitement de leurs données à caractère personnel.

Le groupe de travail avait enfin émis l'idée de fournir des références plus détaillées aux droits d'accès et de recours et avait exprimé son désaccord vis-à-vis de l'extension de la période de conservation par rapport à l'accord de 2005. Il a également émis le souhait que les autorités auxquelles les données peuvent être transférées figurent dans une liste jointe à l'accord ou ses annexes. La négociation de ce type d'accords avec les États-Unis a été complexe, car si les Européens et les Américains s'accordent sur le grand intérêt de cette coopération en matière d'échange de données en faveur de la lutte contre le terrorisme et la criminalité transfrontalière, des désaccords substantiels existent quant au niveau de protection à garantir en matière de données à caractère personnel.

Sous-section 4 – Le Contrôleur européen de la protection des données, une autorité de contrôle indépendante investie dans la protection des droits fondamentaux

Le Contrôleur européen de la protection des données (ci-après CEPD) est l'autorité de contrôle indépendante des institutions européennes qui veille sur la protection des données personnelles. Le CEPD a joué un rôle important dans la mise en avant de la protection des données personnelles des passagers aériens.

§ 1 – Le Contrôleur européen de la protection des données personnelles, un garde-fou devant les institutions européennes

Le CEPD a été institué par le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données⁹⁵³. Ce texte avait pour objectif de protéger le traitement de données à caractère personnel effectué par les institutions et organes de l'Union européenne. C'est dans ce contexte qu'il instaura une autorité de contrôle indépendante chargée de surveiller l'application de ses dispositions.

⁹⁵³ Agence des droits fondamentaux de l'Union européenne, *Manuel de droit européen en matière de protection des données*, éditions 2018, avril 2018, p. 41.

Le CEPD a été investi de pouvoirs de contrôle du traitement des données à caractère personnel au sein des institutions et organes de l'Union ainsi que d'entendre et d'enquêter sur les réclamations dont l'objet est une violation alléguée des règles relatives à la protection des données⁹⁵⁴. Il peut ainsi ordonner au responsable du traitement et au sous-traitant de lui communiquer toute information dont il a besoin pour l'accomplissement de ses missions ; mener des enquêtes sous la forme d'audits sur la protection des données ; notifier au responsable du traitement ou au sous-traitant une violation alléguée du présent règlement ; obtenir du responsable du traitement et du sous-traitant l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'accomplissement de ses missions ; obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation de traitement et à tout moyen de traitement, conformément au droit de l'Union⁹⁵⁵.

Le contrôleur a également pour mission de conseiller les institutions et organes européens dans tous les domaines concernant le traitement de données personnelles, notamment en procédant à des consultations sur des propositions législatives et en surveillant les évolutions qui ont une incidence sur la protection des données. Le CEPD peut conseiller les personnes concernées sur l'exercice de leurs droits mais aussi le responsable du traitement conformément à la procédure de consultation préalable ; émettre, de sa propre initiative ou sur demande, des avis à l'attention des institutions et organes de l'Union ainsi que du public sur toute question relative à la protection des données à caractère personnel ; adopter des clauses types de protection des données et d'autres actions visées par le règlement⁹⁵⁶.

À ces missions de supervision et de consultation s'ajoute une mission de coopération : le CEPD est tenu de coopérer avec les autorités nationales de protection des données ainsi qu'avec les organes de contrôle établis dans le cadre de l'ancien troisième pilier de l'Union en vue d'améliorer l'application cohérente des règles de protection des données.

Le 10 janvier 2017, la Commission européenne a présenté une proposition de nouveau règlement relatif au traitement des données par les institutions européennes dont le but était de proposer un nouveau règlement qui abrogeait le règlement 45/2001. La révision de ce

⁹⁵⁴ Ibidem

⁹⁵⁵ 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, article 58, alinéa 1.

⁹⁵⁶ Ibidem.

règlement devait le mettre en conformité avec le RGPD, comme ce fut le cas de la réforme de la directive « vie privée et communications électroniques »⁹⁵⁷.

La révision a débouché sur le 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, qui a abrogé le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE.

L'article 52, alinéa 2 de ce nouveau règlement précise que le Contrôleur européen de la protection des données est chargé « de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union »⁹⁵⁸. L'alinéa 3 du même article ajoute un autre objectif puisque le CEPD le charge également « de contrôler et d'assurer l'application des dispositions du présent règlement et de tout autre acte de l'Union concernant la protection des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel effectués par une institution ou un organe de l'Union, ainsi que de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel »⁹⁵⁹.

Le contrôleur européen de la protection des données est nommé d'un commun accord par le Parlement européen et le Conseil, pour une durée de cinq ans, sur la base d'une liste établie par la Commission à la suite d'un appel public à candidatures. Les personnes intéressées, au sein de l'Union européenne, peuvent soumettre leur candidature grâce à cet appel à candidatures. La Commission établit une liste qui est publique et comporte au moins trois candidats. La commission compétente au sein du Parlement européen, sur la base de la liste établie par la Commission, a le pouvoir d'organiser une audition afin d'être en mesure d'émettre une préférence vis-à-vis d'une candidature⁹⁶⁰.

Le mandat du CEPD est renouvelable une fois⁹⁶¹ et ses fonctions peuvent prendre fin dans le cas où il est remplacé, en cas de démission ou s'il est déclaré démissionnaire ou mis à la retraite d'office⁹⁶².

⁹⁵⁷ Ibid.

⁹⁵⁸ 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, article 52, alinéa 2.

⁹⁵⁹ Ibidem, article 52, alinéa 3.

⁹⁶⁰ Ibid., article 53, alinéa 1.

⁹⁶¹ Ibid., article 53, alinéa 3.

Siégeant à Bruxelles⁹⁶³, le CEPD exerce une fonction qui est équivalente à celle du juge de la Cour au regard de ses conditions en termes de traitement, d'indemnités, de pension d'ancienneté et d'autres avantages⁹⁶⁴. Le CEPD est assisté par un secrétariat dont les fonctionnaires et autres agents sont nommés par le Contrôleur qui est considéré comme leur supérieur hiérarchique⁹⁶⁵.

Libre de toute influence extérieure, le Contrôleur exerce ses missions et ses pouvoirs en toute indépendance, sous la garantie du droit européen en la matière⁹⁶⁶. Il ne reçoit ni ne sollicite d'instructions d'aucunes entités. Lui et son secrétariat sont tenus de respecter les principes d'honnêteté et de délicatesse dans l'exercice de leurs fonctions et de leurs avantages. Ils sont également tenus de respecter, pendant toute la durée de leur mandat et après sa cessation, le principe du secret professionnel en ce qui concerne toutes les informations confidentielles dont ils ont eu connaissance lors de l'exercice de leurs fonctions officielles⁹⁶⁷.

Conformément à l'article 57 du règlement (UE) 2018/1725, le Contrôleur européen de la protection des données (CEPD) est chargé d'une gamme variée de missions, notamment de veiller à l'application du règlement par les institutions et organes de l'Union, à l'exception du traitement des données par la Cour dans le cadre de ses fonctions juridictionnelles. Il joue également un rôle crucial dans la sensibilisation du public, en informant sur les risques, les règles, les garanties et les droits relatifs au traitement des données à caractère personnel. En outre, il encourage les responsables du traitement et les sous-traitants à respecter les obligations imposées par le règlement⁹⁶⁸.

Le CEPD est également responsable du traitement des réclamations formulées par les personnes concernées, les organismes, les organisations ou les associations. Il examine les réclamations, informe les plaignants de l'état d'avancement de l'enquête et de ses résultats dans un délai raisonnable, tout en veillant à la coordination avec d'autres autorités de contrôle si nécessaire. En parallèle, il mène des enquêtes sur l'application du règlement, y compris sur la base d'informations fournies par d'autres autorités de contrôle ou des autorités publiques.

Par ailleurs, le CEPD conseille les institutions et organes de l'Union sur les questions législatives et administratives relatives à la protection des données personnelles, que ce soit de

⁹⁶² Ibid., article 53, alinéa 4.

⁹⁶³ Ibid., article 54, alinéa 6.

⁹⁶⁴ Ibid., article 54, alinéa 1.

⁹⁶⁵ Ibid., article 54, alinéa 4.

⁹⁶⁶ Ibid., article 55.

⁹⁶⁷ Ibid., article 56.

⁹⁶⁸ Ibid., article 57, alinéa 1.

sa propre initiative ou à la demande. Il surveille également les évolutions pertinentes, en particulier dans le domaine des technologies de l'information et des communications, et maintient une liste relative aux analyses d'impact sur la protection des données.

Enfin, le CEPD participe aux activités du Comité européen de la protection des données, assure son secrétariat, autorise les clauses contractuelles, et tient des registres internes des violations du règlement ainsi que des mesures prises. Il peut également accomplir toute autre mission relative à la protection des données à caractère personnel et établir son règlement intérieur⁹⁶⁹.

Par ailleurs, dans le cadre de ses missions, le CEPD est amené à faciliter l'introduction des réclamations par la mise à disposition d'un formulaire de réclamation⁹⁷⁰. Cette action est réalisée par voie électronique, sans que d'autres moyens de communication ne soient exclus⁹⁷¹. Les personnes qui s'adressent au CEPD ne sont pas appelées à payer pour ces réclamations⁹⁷². Dans le cas où les demandes sont « manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif »⁹⁷³, le CEPD peut refuser d'y donner suite. C'est à ce dernier qu'il incombe de démontrer le caractère manifestement infondé ou excessif de la demande.

Le CEPD dispose de pouvoirs étendus pour adopter des mesures correctrices⁹⁷⁴. Il peut notamment avertir un responsable du traitement ou un sous-traitant lorsque les opérations de traitement envisagées sont susceptibles de contrevenir aux dispositions du règlement. En cas de violation avérée, le CEPD peut rappeler à l'ordre le responsable ou le sous-traitant concerné et, si nécessaire, alerter le Parlement européen, le Conseil, et la Commission européenne.

En outre, le CEPD peut ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes des personnes concernées pour l'exercice de leurs droits conformément au règlement. Il peut également exiger la mise en conformité des opérations de traitement avec les dispositions du règlement dans des conditions spécifiques et dans un délai déterminé. En cas de violation de données à caractère personnel, le CEPD peut ordonner au responsable de communiquer cette violation à la personne concernée⁹⁷⁵.

⁹⁶⁹ Ibid.

⁹⁷⁰ Ibid., article 57, alinéa 2.

⁹⁷¹ Ibid.

⁹⁷² Ibid., article 57, alinéa 3.

⁹⁷³ Ibid., article 57, alinéa 4.

⁹⁷⁴ Ibid., article 58.

⁹⁷⁵ Ibid.

Le CEPD a également le pouvoir d'imposer des limitations temporaires ou définitives, y compris des interdictions, sur le traitement des données. Il peut ordonner la rectification, l'effacement ou la limitation du traitement des données personnelles, et imposer des amendes administratives en cas de non-conformité d'une institution ou d'un organe de l'Union. Enfin, il peut ordonner la suspension des flux de données vers un destinataire situé dans un État membre, un pays tiers ou une organisation internationale.

§ 2 – Le Contrôleur européen, une autorité garante de la protection des données personnelles des passagers aériens

Le Contrôleur européen de la protection des données (CEPD) a exprimé des critiques significatives dès les débuts concernant l'utilisation des données personnelles des passagers aériens. Dans son avis du 1er mai 2008⁹⁷⁶, il a soulevé des préoccupations sur la nécessité d'implémenter un système PNR. Ces réserves rejoignent celles formulées par l'Agence des droits fondamentaux dans son avis du 3 décembre 2008 et par le Groupe de l'article 29 sur la protection des données dans son avis du 5 décembre 2007⁹⁷⁷.

Le CEPD insistait notamment sur l'insuffisance d'éléments d'information et de retours d'expérience qui puissent démontrer la nécessité et l'utilité de la collecte des données des passagers aériens à des fins répressives. Pour ce dernier, l'absence de preuve de l'intérêt du système serait d'autant plus problématique que la collecte indifférenciée des données des dossiers passagers de tous les voyageurs des États membres de l'Union européenne est susceptible de mettre en péril le respect des droits fondamentaux des citoyens européens⁹⁷⁸.

Les critiques du CEPD se sont concentrées sur la technique du profilage qui bâtit des hypothèses de risques à partir de données personnelles ne caractérisant pourtant pas une infraction⁹⁷⁹. Le profilage permet l'élaboration de modèles de comportement et de déplacement qui conduisent à fonder des décisions possiblement préjudiciables à l'encontre d'individus qui auront beaucoup de mal, par la suite, à se défendre contre des décisions prises à leur encontre⁹⁸⁰.

⁹⁷⁶ CEPD, avis du 1er mai 2008 sur la proposition de directive relative à l'utilisation des données PNR, 2008/C 102/01.

⁹⁷⁷ S. SUTOUR et Y. DETRAIGNE, « Rapport n° 401 : La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives », Sénat, Commission des lois, 13 mai 2009, en ligne à URL : <http://www.senat.fr/ue/pac/E6014.html> consulté en ligne le 23 mars 2023.

⁹⁷⁸ CEPD, avis du 1er mai 2008 sur la proposition de directive relative à l'utilisation des données PNR, 2008/C 102/01.

⁹⁷⁹ Ibidem

⁹⁸⁰ Ibid.

Les autres critiques émises par le CEPD portaient sur le système élaboré par la Commission européenne, notamment sur le droit applicable en matière de protection des données personnelles concernant le droit d'accès, de rectification, de transferts des données vers des pays tiers qui est jugé imprécis, voire inexistant. Par ailleurs, la durée de conservation des données personnelles des passagers aériens était considérée comme excessive⁹⁸¹.

Le CEPD s'est également prononcé sur la proposition d'accord de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers au ministère américain de la sécurité intérieure dans un avis en date du 9 décembre 2011⁹⁸².

Le 28 novembre 2011, la Commission avait adopté une proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis sur l'utilisation et le transfert des données des dossiers passagers. Le 2 novembre 2011, le Contrôleur a été consulté, de manière informelle, sur le projet de proposition d'accord PNR, dans le cadre d'une procédure accélérée. Dans un premier temps, le CEPD a émis de brèves observations, dans un avis du 11 novembre 2011.

L'avis du 9 décembre 2011⁹⁸³ est venu compléter ces observations initiales sur la proposition d'accord PNR qu'il a rendu publiques. Le CEPD a accueilli favorablement les garanties prévues dans le nouvel accord sur la sécurité et le contrôle des données des passagers aériens ainsi que les améliorations par rapport à l'accord de 2007. Toutefois, il a rappelé que certaines préoccupations demeuraient.

Tout d'abord, le CEPD considéra que la période de conservation de 15 ans était excessive. Selon lui, les données devaient être effacées immédiatement après leur analyse, ou après une période maximale de 6 mois. Il jugea aussi la limitation de la finalité de traitement comme étant trop large. Il fit aussi observer que les données PNR ne devraient être utilisées que dans le cadre de la lutte contre les infractions terroristes ou d'une liste bien déterminée de crimes transnationaux graves.

Par ailleurs, le CEPD considéra la liste des données devant être transférées au Department of Homeland Security (DHS) était disproportionnée. Pour lui, elle comportait trop de champs

⁹⁸¹ Ibid.

⁹⁸² Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure, 9 décembre 2011, (2012/C 35/03).

⁹⁸³ Ibidem

ouverts. Il recommandait ainsi qu'elle soit réduite et qu'en soient exclues les données sensibles. En ce qui concerne les méthodes de traitement, il fit remarquer qu'il existait des exceptions à la méthode « push » et que celles-ci devaient être retirées. Il recommandait également que les autorités américaines ne puissent pas être en mesure d'accéder directement aux données, à travers la méthode « pull ».

L'autorité européenne a également noté des restrictions sur l'exercice des droits des personnes concernées. Ces limitations, auxquelles le CEPD fait référence, touchent la capacité des individus à exercer pleinement leurs droits en matière de protection des données, notamment le droit de recours juridictionnel effectif. Parmi ces restrictions figurent l'absence de mécanismes de recours efficaces et le manque de transparence quant à l'utilisation des données personnelles. Le CEPD défend le principe que chaque citoyen doit pouvoir exercer un droit de recours juridictionnel effectif et obtenir réparation en cas de violation de ses droits⁹⁸⁴.

Enfin, le CEPD a conclu que le ministère de l'Intérieur américain, le DHS, ne devait pas transférer les données personnelles à d'autres autorités américaines ou à des pays tiers, à moins qu'ils ne garantissent un niveau de protection équivalent de protection.

Par ailleurs, le Contrôleur européen de la protection des données avait jugé que « tout accord légitime prévoyant le transfert massif de données personnelles de passagers vers des pays tiers doit remplir des conditions strictes. Malheureusement, de nombreuses préoccupations exprimées par le CEPD et les autorités nationales de protection des données des États membres n'ont pas été rencontrées. Il en va de même des conditions posées par le Parlement européen pour donner son consentement »⁹⁸⁵.

Ces débats sont intervenus dans un contexte particulier pour les dossiers passagers puisque les transferts de données PNR entre les États-Unis et l'Union européenne s'opéraient à l'époque sur la base de l'accord PNR de 2007. Or, celui-ci s'appliquait de manière provisoire étant donné que le Parlement européen avait décidé de ne pas donner son consentement. La non-approbation par le Parlement d'un nouvel accord signifiait que l'accord devait être renégocié⁹⁸⁶.

⁹⁸⁴ L'article 47 de la Charte des droits fondamentaux de l'Union européenne garantit à toute personne le droit à un recours effectif devant un tribunal et le droit à un procès équitable.

⁹⁸⁵ Communiqué de presse, « Le CEPD rend un avis sur le nouvel accord UE-USA sur les données des dossiers passagers (données PNR) », *Union européenne*, le 13 décembre 2011.

⁹⁸⁶ Ibidem

Dans le cadre des récents débats autour des accords PNR, une attention particulière a été portée sur les procédures de consultation prévues par le règlement général sur la protection des données (RGPD). À propos de l'accord entre l'Union européenne et les États-Unis sur le transfert des données transatlantiques du 25 mars 2022⁹⁸⁷, le CEPD a rapidement souligné que sa consultation était obligatoire avant toute décision de la part de la Commission, conformément à l'article 64 du RGPD, qui précise les cas où l'avis du Comité européen doit être sollicité par les autorités compétentes⁹⁸⁸.

Tout en saluant l'accord entre la Commission et les États-Unis, le CEPD a néanmoins souligné l'existence de « défis significatifs » concernant les transferts de données depuis l'Espace économique européen vers les États-Unis⁹⁸⁹. Le CEPD a également précisé que, malgré les « propositions juridiques concrètes » qu'il attend, l'annonce de l'accord ne constituait pas encore « un cadre légal » suffisant pour que les utilisateurs et exportateurs de données puissent s'y appuyer pour leurs transferts vers les États-Unis⁹⁹⁰.

Le CEPD a annoncé se montrer exigeant sur la manière dont les nouveaux accords « assureront que la collecte de données personnelles à des fins de sécurité nationale » soit limitée au strict nécessaire et proportionnée. Le Comité semble sensible à la question des mécanismes de recours indépendants qui devront respecter le droit des citoyens européens à un recours effectif et à un procès équitable. En particulier, il semble que l'on espère qu'une nouvelle autorité au sein de ce mécanisme pourra accéder aux informations pertinentes, y compris aux données personnelles, dans le cadre de ses fonctions et aura la capacité de prendre des décisions contraignantes pour les services de renseignement⁹⁹¹.

Le 7 octobre 2022, le président américain Biden a signé un décret exécutif visant à renforcer les garanties encadrant les activités du renseignement américain en matière de transfert des données⁹⁹². Ce décret met en œuvre les engagements pris les États-Unis en mars 2022, intégrant ces mesures dans le droit américain. Vis-à-vis des données personnelles des citoyens européens transférées aux États-Unis, le décret prévoyait d'abord des garanties contraignantes

⁹⁸⁷ J. CHEMINAT, « USA et UE signent un accord pour succéder au Privacy Shield », *Le monde informatique*, 28 mars 2022.

⁹⁸⁸ CNIL, Déclaration 01/2022 du Comité européen de la protection des données sur l'annonce d'un accord de principe sur un nouveau cadre transatlantique pour la protection des données, 6 avril 2022.

⁹⁸⁹ Ibidem

⁹⁹⁰ Ibid.

⁹⁹¹ Ibid.

⁹⁹² Executive Order to Implement the European Union-U.S. Data Privacy Framework, 22 octobre 2022.

limitant l'accès aux données personnelles par les autorités de renseignement étasunien à ce qui est nécessaire et proportionné pour la protection de la sécurité nationale⁹⁹³.

Le décret envisageait également la mise en place d'un mécanisme de recours indépendant et impartial, à deux niveaux, pour les personnes concernées. D'une part, un officier de protection des libertés civiles rattaché au bureau du directeur du renseignement national (CLPO) qui peut mener une enquête initiale sur les plaintes admissibles reçues. Cet officier de protection peut déterminer si les garanties renforcées, notamment par le décret ou les lois américaines applicables, ont été enfreintes et, le cas échéant, peut indiquer les mesures correctives appropriées. D'autre part, une Cour de révision de la protection des données (DPRC) a été instaurée pour assurer un contrôle indépendant des décisions de la CPLD, enquêter et résoudre les plaintes concernant l'accès à leurs données par les autorités de sécurité nationale des États-Unis⁹⁹⁴.

Enfin, le décret exécutif du président américain obligea les agences de renseignement américaines à réévaluer leurs politiques et procédures pour mettre en œuvre ces nouvelles garanties.

Certaines étapes sont nécessaires avant d'obtenir la publication officielle par la Commission d'une décision d'adéquation avec les États-Unis. L'avis du Comité européen de la protection des données, qui a indiqué se concentrer sur la garantie que la collecte de données à caractère personnel à des fins de sécurité nationale est limitée au strict nécessaire et proportionnée, a d'abord été obtenu⁹⁹⁵. Ensuite, un feu vert est requis d'un comité composé de représentants des États membres de l'Union européenne.

Ces évolutions juridiques n'ont pas manqué de faire réagir les spécialistes de la protection des données personnelles en Europe. Max Schrems, le juriste autrichien à l'origine des deux recours portés devant la CJUE en matière de protection des données personnelles, a contesté ce nouveau décret au motif que « l'Union européenne et les États-Unis sont désormais d'accord sur l'utilisation du mot 'proportionné', mais ne semblent pas s'accorder sur sa signification. Au final, c'est la définition de la CJUE qui prévaudra — ce qui risque de rendre caduque toute décision de l'UE. La Commission européenne ferme une fois de plus les yeux sur le droit américain, pour permettre de continuer à espionner les Européens ».

⁹⁹³ Ibidem.

⁹⁹⁴ M. PONTRUCHER, « Accord entre l'Union européenne et les États-Unis sur le transfert de données : jamais deux sans trois ? », *Digitemis*, 22 octobre 2022.

⁹⁹⁵ CNIL, Transfert de données vers les États-Unis : le CEPD rend son avis sur le projet de décision d'adéquation de la Commission européenne, 21 mars 2023, en ligne à URL : <https://www.cnil.fr/fr/transfert-de-donnees-vers-les-etats-unis-le-cepd-rend-son-avis-sur-le-projet-de-decision-dadequation>, consulté le 8 mai 2024.

Pour ce dernier, la divergence dans l'acception du principe de proportionnalité fragilise cet accord au détriment de la protection des données personnelles des citoyens européens⁹⁹⁶. Par ailleurs, le juriste autrichien a contesté le statut de la nouvelle Cour de révision de la protection des données. Selon ce dernier, cette juridiction ne serait pas suffisamment indépendante dans la mesure où elle relève de la branche exécutive du Gouvernement américain. Conséquemment, les citoyens européens ne pourront pas bénéficier d'un recours judiciaire tel que prévu par la Charte des droits fondamentaux⁹⁹⁷. La fragilité de cet accord, s'agissant du droit au recours des citoyens, laisse à prévoir que la CJUE sera de nouveau saisie à ce sujet dans les années qui viennent.

L'éventualité d'une nouvelle saisine de la CJUE dans les années à venir concernant le droit au recours des citoyens soulève des questions cruciales quant à la protection des données à caractère personnel, notamment dans le contexte des différentes fonctions exercées par cette institution et les spécificités de leur traitement. Cette dernière peut être amenée à traiter des données à caractère personnel dans l'exercice de ses fonctions ainsi que dans l'exercice d'autres fonctions. Selon la nature des fonctions concernées, la protection des données à caractère personnel présente des caractéristiques spécifiques. Dans l'exercice de leurs fonctions juridictionnelles, les juridictions européennes (la Cour de justice et le Tribunal) sont contraintes à des exigences spécifiques découlant de la nature de leurs missions, notamment la nécessité de respecter les principes d'indépendance et de transparence judiciaire. Le juge européen semble être conscient que ces données sont susceptibles de se recouper, exposant les informations relatives à la vie privée et données personnelles des voyageurs, bien que toutes les données personnelles ne concernent pas la vie privée.

Toujours est-il que les juridictions européennes semblent mettre en avant les moyens juridiques de protection, qui peuvent se compléter ou être distincts. Le juge européen semble considérer qu'il est nécessaire de les examiner dans leur diversité. En effet, le traitement des données personnelles des passagers aériens doit être destiné au service d'un itinéraire de voyage plus sûr et plus sécurisé. Bien que le droit à la protection des données personnelles ne soit pas un droit absolu, le juge européen semble considérer ce droit par rapport à sa fonction dans la société et mis en balance avec d'autres droits fondamentaux selon le principe de proportionnalité⁹⁹⁸.

⁹⁹⁶ Ibid.

⁹⁹⁷ Ibid.

⁹⁹⁸ Ibid.

Après avoir examiné les enjeux liés aux transferts de données entre l'Union européenne et les États-Unis, il convient maintenant de se tourner vers le cadre spécifique des accords entre l'Union européenne et le Canada en matière de dossiers passagers. Le CEPD également exprimé sur l'accord entre l'Union européenne et le Canada pour le transfert de données personnelles des passagers aériens qui comportait à ses yeux des différences fondamentales au regard de l'accord conclu avec les États-Unis. Premièrement, l'accord euro-canadien a exclu le système de traitement « pull » au profit d'un système de type « push ». Cela a eu pour conséquence que les compagnies aériennes qui opèrent dans l'espace européen sont en mesure de contrôler les transferts de données des dossiers passagers qui partent vers le Canada⁹⁹⁹.

Deuxièmement, l'autorité européenne constata que les engagements pris par les autorités canadiennes avaient un caractère contraignant. Cela a eu pour conséquence de donner à la proposition d'accord PNR un caractère plus équilibré par rapport à l'accord conclu avec les autorités américaines¹⁰⁰⁰. Troisièmement, l'avis nota que la liste des données personnelles des passagers aériens à transférer était plus limitée que celle prévue par l'accord euro-américain. En outre, elle ne contenait pas de « catégories ouvertes » de données « passagers » que le contrôleur craignait parce qu'elles peuvent révéler des informations sensibles¹⁰⁰¹.

Ainsi, cet accord posa les bases d'un système législatif de meilleure protection des données personnelles des passagers aériens donc une meilleure protection de leurs droits fondamentaux comme le droit à la protection de la vie privée et le droit à la protection des données à caractère personnel. Cette amélioration se traduisit également par la mise en place d'un contrôle réalisé par un commissaire indépendant à la protection de la vie privée.

Toutefois, le droit canadien n'offrait pas, selon le CEPD¹⁰⁰², une totale protection des données à caractère personnel aux citoyens européens. C'est ce qui justifia la conclusion d'un accord qui puisse permettre aux autorités canadiennes de combler cette lacune. L'organe européen avait émis le souhait que le passager aérien européen puisse avoir accès aux textes des instruments législatifs canadiens et qu'il dispose d'un accès réel aux voies de recours¹⁰⁰³. C'est pourquoi il a approuvé la procédure par laquelle le commissaire à la protection de la vie privée du Canada a la possibilité d'examiner les plaintes qui lui sont transmises par les

⁹⁹⁹ Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion d'un accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations anticipées sur les voyageurs (API)/dossiers passagers (PNR), (2005/C 218/06), 15 juin 2005.

¹⁰⁰⁰ Ibidem

¹⁰⁰¹ Ibid.

¹⁰⁰² Ibid.

¹⁰⁰³ Ibid.

autorités de protection des données de tout État membre pour le compte d'un résident de l'Union européenne. Selon le contrôleur européen, ce type de procédure pourrait même se révéler, en pratique, plus efficace qu'un hypothétique droit formel d'agir devant les tribunaux canadiens reconnu aux résidents européens¹⁰⁰⁴.

La reconnaissance de ces éléments positifs présents dans la proposition de décision du Conseil relative à la conclusion d'un accord entre la Communauté européenne et le Gouvernement du Canada sur le traitement des données des dossiers passagers a amené le CEPD à approuver les principaux éléments de l'accord négocié entre les autorités européennes et canadiennes¹⁰⁰⁵.

§ 3 – Le rôle du CEPD dans le cadre des négociations sur l'accord entre l'Union européenne et le Japon

Situé en Asie de l'Est, le Japon est une monarchie constitutionnelle parlementaire¹⁰⁰⁶. La Constitution japonaise a été adoptée en 1947 alors que le pays était sous occupation américaine, après la Seconde guerre mondiale. La Constitution japonaise établit les principes fondamentaux de gouvernement et garantit les droits individuels. Bien que l'Empereur du Japon soit une figure de prestige, le pouvoir réel réside dans les mains du gouvernement élu. L'Empereur n'a pas de pouvoirs politiques significatifs et joue un rôle principalement symbolique.

Le Parlement japonais, dénommé Diète nationale (Kokkai)¹⁰⁰⁷, est composé de deux chambres : la Chambre des représentants (Shūgiin) et la Chambre des conseillers (Sangiin). Les membres des deux chambres sont élus par les citoyens japonais. L'exécutif japonais est dirigé par le Premier ministre qui est le chef du parti politique dominant à la Chambre des représentants. Le Premier ministre est nommé par l'Empereur mais doit être approuvé par la Diète. Le Japon possède un système judiciaire indépendant qui est basé sur la loi et la Cour suprême du Japon est la plus haute instance judiciaire du pays.

Le droit japonais¹⁰⁰⁸ est principalement de nature civile, autrement dit son système juridique repose sur la codification de lois écrites, mais il incorpore aussi des éléments du droit

¹⁰⁰⁴ Ibid.

¹⁰⁰⁵ Ibid.

¹⁰⁰⁶ Constitution du Japon, promulguée le 3 novembre 1946, entrée en vigueur le 3 mai 1947, en ligne à URL : <https://mjp.univ-perp.fr/constit/jp1946.htm> consulté le 1er septembre 2023.

¹⁰⁰⁷ La Diète nationale du Japon, 16 pages, en ligne à URL : [https://www.shugiin.go.jp/internet/itdb_english.nsf/html/statics/english/kokkaiannai_f2202.pdf/\\$File/kokkaianna_i_f2202.pdf](https://www.shugiin.go.jp/internet/itdb_english.nsf/html/statics/english/kokkaiannai_f2202.pdf/$File/kokkaianna_i_f2202.pdf) consulté le 1er septembre 2023.

¹⁰⁰⁸ R. SEROUSSI, « Le droit japonais », Introduction au droit comparé, Dunod, pp. 173 à 181, 2009, en ligne à URL : <https://www.cairn.info/introduction-au-droit-compare--9782100519491-page-173.htm> consulté le 1er septembre 2023.

coutumier et a été influencé par le droit continental à la suite d'une réforme d'après-guerre¹⁰⁰⁹. Le code civil japonais a ainsi été influencé par les modèles français et allemand dans plusieurs domaines tels que la propriété, les contrats et les successions. Ce droit incorpora des éléments du droit coutumier, notamment dans le domaine du droit de la famille. En effet, les juges japonais considèrent souvent les normes sociales et culturelles traditionnelles lorsqu'ils prennent des décisions en matière d'affaires familiales.

Aujourd'hui, le Japon est un acteur actif dans le domaine du droit international. Le pays a ratifié de nombreuses conventions et traités internationaux. Le droit international joue un rôle important dans les relations extérieures du Japon et dans la réglementation de diverses questions telles que les droits de l'Homme et le commerce international.

Adopté en 2003, puis amendé en 2007, le Protection of Personal Information Act (APPI) est le texte japonais de référence en matière de protection des données à caractère personnel. Son article 1^{er} indique qu'il vise à « protéger les droits et les intérêts des individus tout en considérant l'utilité des informations personnelles, notamment pour la création de nouvelles industries, la réalisation d'une société économique dynamique et une meilleure qualité de vie pour la population japonaise »¹⁰¹⁰. Dans ce cadre, il régleme la collecte, l'utilisation et le transfert des données « personnelles », « personnelles sensibles » et « anonymisées ». Aussi, ce texte prévoit que le consentement de l'utilisateur est requis préalablement pour la collecte de ses données personnelles, à nouveau, en cas de modification substantielle de leur utilisation, ainsi qu'en cas de transfert vers l'étranger ou à un tiers, à l'exception des pays qui disposent d'une reconnaissance d'adéquation avec le Japon. La loi prévoit que l'utilisateur doit être informé de l'affectation de ses données.

Cette législation japonaise a également créé la Personal Information Protection Commission (PPC) dont l'objet est de superviser la mise en œuvre de la loi et des normes que celle des normes internationales de protection des données à caractère personnel. Le cas échéant, et à la suite d'enquêtes internes, cette commission peut exiger des réformes vis-à-vis des organismes mis en cause pour non-respect desdites normes, sous peine de sanctions par les tribunaux. Ainsi, le non-respect des dispositions de la loi japonaise expose les justiciables à six mois de prison et/ou à des amendes de 2500 à 3000 euros. Cette entité a également pour mission de

¹⁰⁰⁹ S. SERVERIN, « La légitimité de la Constitution dans la doctrine constitutionnelle japonaise », Mémoires et responsabilités de guerre. Les procès de Tôkyô et de La Haye, Droit et cultures, pp. 179-198, 2009, en ligne à URL : <http://journals.openedition.org/droitcultures/2191> consulté le 1er septembre 2023.

¹⁰¹⁰ Direction générale du Trésor, « La protection des données personnelles au Japon », 8 mai 2019, en ligne à URL : <https://www.tresor.economie.gouv.fr/Articles/2019/05/08/la-protection-des-donnees-personnelles-au-japon> consulté en ligne le 25 mars 2023.

connaître l'adéquation des systèmes de protection de pays tiers, tout comme le fait la Commission européenne dans le cadre de l'article 103 du RGPD¹⁰¹¹.

La réforme de la loi japonaise sur la protection des données à caractère personnel est devenue effective à compter du 30 mai 2017¹⁰¹². Elle a attiré l'attention des sociétés françaises opérant en Japon au moment où les sociétés japonaises étaient occupées par leur mise en conformité avec le droit européen de la protection des données à caractère personnel, dont le RGPD est le texte phare.

Le 1^{er} février 2019, un Accord de partenariat économique (APE) entre l'Union européenne et le Japon a permis aux deux parties de mettre en adéquation leurs règles en matière de traitement de données à caractère personnel. Ce cadre juridique a consolidé les rapports entre les deux pays en matière de politique étrangère et de promotion des valeurs telles que la démocratie, les droits de l'Homme, le multilatéralisme et l'État de droit¹⁰¹³. Dans le cas d'un différend sur le territoire japonais, le PCC dispose de pouvoirs de médiation, d'enquêtes et, le cas échéant, peut enjoindre à l'organisme traitant les données d'adopter des réformes internes. En dernier recours, le juge japonais est compétent pour juger de la bonne application des règles additionnelles d'adéquation qui ont été adoptées en 2018.

Les efforts du Japon s'inscrivent dans le cadre d'une politique générale qui vise à promouvoir la protection des données à caractère personnel, y compris dans le domaine de la politique internationale. Dès décembre 2016, le Japon avait adopté le système CBPR (Cross Border Privacy Rules system) de la Coopération économique pour l'Asie-Pacifique (en anglais : Asia-Pacific Economic Cooperation, APEC). Ce dernier est comparable au système établi entre l'Union européenne et les États-Unis, le Privacy Shield. Il rend possible le transfert frontalier de données personnelles, sans consentement additionnel de l'utilisateur, ni démarche administrative supplémentaire, aux entreprises certifiées. En effet, une certification est accordée par les autorités nationales indépendantes, le TRUSTE aux États-Unis, le JIPDEC au Japon, lorsqu'un niveau minimal de protection des données à caractère personnel est garanti par l'entité en question¹⁰¹⁴.

¹⁰¹¹ Ibidem

¹⁰¹² D. LE DOUSSAL, S. HATANO, « Réforme de la loi sur la protection des informations personnelles au Japon », CCI France Japon, Analyses & Études, 17 mai 2017, en ligne à URL : <https://www.cci.fr/publications/actus/n/news/reforme-de-la-loi-sur-la-protection-des-informations-personnelles-au-japon.html> consulté en ligne le 25 mars 2023.

¹⁰¹³ Vie publique, « Un accord commercial UE-Japon : entrée en vigueur le 1^{er} février 2019 », 30 janvier 2019.

¹⁰¹⁴ D. LE DOUSSAL, S. HATANO, « Réforme de la loi sur la protection des informations personnelles au Japon », CCI France Japon, Analyses & Études, 17 mai 2017, en ligne à URL :

Depuis 2016, le Japon a investi le champ de la coopération internationale et l'échange de bonnes pratiques dans le domaine des données à caractère personnel. C'est dans ce contexte que le PCC a adhéré au Global Privacy Enforcement Network (GPEN). Créé en 2007 sur recommandation de l'OCDE, ce dernier encourage ses membres à coopérer afin d'améliorer la protection et le transfert frontalier des données, au moyen d'études par exemple. La Commission japonaise a également rejoint les Asia Pacific Privacy Authorities (APPA), un groupe d'échanges entre autorités nationales de régulation, dont l'objet est de former des partenariats et de proposer des recommandations. Dans cette dynamique, le Japon a adopté en 2016 le plan New Initiatives for Ensuring Smooth Cross-Border Personal Data Flows, visant à renforcer le dialogue sur ce sujet avec l'Union européenne et les États-Unis¹⁰¹⁵.

Enfin, les autorités japonaises ont décidé de faire de la bonne gouvernance mondiale l'une des priorités de leur présidence du G20 en mettant en avant le concept de Data Free Flow with Trust. Ce dernier vise à encourager la circulation transfrontalière des données tout en garantissant leur protection suffisante afin de développer une relation de confiance entre les différents acteurs, dont les États, les utilisateurs et les entreprises. Le Gouvernement japonais a lancé Osaka Track, un processus qui vise à intensifier les efforts pour développer des règles internationales sur l'économie numérique, en particulier sur les flux de données et le commerce électronique, tout en promouvant des protections renforcées pour la propriété intellectuelle, les données personnelles et la cybersécurité, dans le cadre de l'Organisation mondiale du commerce¹⁰¹⁶.

Récemment, le CEPD s'est prononcé, dans un avis, sur le mandat de négociation d'un accord entre l'Union européenne et le Japon pour le transfert et l'utilisation de données des dossiers passagers. La Commission européenne a adopté, le 27 septembre 2019, une recommandation sur une décision du Conseil qui autorise l'ouverture d'un accord entre les autorités européennes et japonaises aux fins du transfert et de l'utilisation de données des dossiers passagers, au titre de la prévention et de la lutte contre les infractions terroristes et les autres formes de crimes transnationaux¹⁰¹⁷. Pour l'Union européenne, le Japon est un « proche partenaire stratégique de l'Union européenne dans la lutte contre le terrorisme et d'autres

<https://www.ccifj.or.jp/publications/actus/n/news/reforme-de-la-loi-sur-la-protection-des-informations-personnelles-au-japon.html> consulté en ligne le 25 mars 2023.

¹⁰¹⁵ Ibidem

¹⁰¹⁶ Digwatch, « The G20 Osaka Track raises controversy », 1er juillet 2019, en ligne à URL : <https://dig.watch/updates/g20-osaka-track-raises-controversy> consulté en ligne le 26 mars 2023.

¹⁰¹⁷ Commission européenne, Recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et le Japon aux fins du transfert et de l'utilisation de données des dossiers passagers (PNR) afin de prévenir et de combattre le terrorisme et d'autres formes graves de criminalité transnationale, 27 septembre 2019.

formes graves de criminalité transnationale »¹⁰¹⁸. Les deux collaborent sur les problématiques de sécurité de leurs citoyens dans le cadre des Nations unies, du G20, du G7 et d'autres enceintes supranationales afin garantir la sécurité de leurs citoyens.

En juillet 2018, l'Union européenne et le Japon ont signé un accord de partenariat stratégique qui, en plus de renforcer leur partenariat global, encourage les deux parties à utiliser les outils à leur disposition, dont les dossiers passagers, afin de prévenir et combattre les infractions terroristes et crimes graves tout en veillant au respect du droit à la protection à la vie privée et la protection des données à caractère personnel¹⁰¹⁹. Bien qu'ils aient été vus comme des avancées, les amendements apportés à cette législation japonaise ne permettaient pas encore de garantir un niveau de protection juridique équivalent à celui du droit européen, plus précisément depuis le RGPD. La loi a notamment opté pour une définition restreinte des « données personnelles sensibles » qui n'incluait pas l'orientation sexuelle et l'appartenance à un syndicat. De plus, elle envisageait des données « anonymisées » sans requérir l'irrévocabilité de l'anonymat ou encore n'exigeait pas des entreprises de communiquer les données personnelles d'un individu, à sa demande, si ces dernières étaient utilisées pendant moins de six mois.

Depuis quelques années, la Commission japonaise pour la protection des données personnelles a entrepris des réformes pour que sa législation se mette au niveau des standards de protection européens et que soit obtenue, *in fine*, une décision d'adéquation avec l'Union européenne. Des négociations ont eu lieu entre Européens et Japonais en vue d'une reconnaissance d'adéquation mutuelle. En septembre 2018, le PCC a adopté une série de dispositions additionnelles visant à faire correspondre le système japonais de protection des données à caractère personnel au cadre de protection européen¹⁰²⁰. Ces réformes n'ont pas estompé les différences qui existent entre les deux systèmes juridiques de protection des données personnelles. Ainsi, à l'inverse du droit européen, la Cour Suprême japonaise n'a pas reconnu le droit à l'oubli dans son arrêt de juillet 2018¹⁰²¹, ni le droit au contrôle de ses propres informations ou le droit pour un individu d'engager une procédure judiciaire afin d'avoir accès à ses données à caractère personnel. Le débat n'est pas clos au Japon où la reconnaissance de ces droits est toujours débattue.

¹⁰¹⁸ Ibidem

¹⁰¹⁹ EU-Japan Strategic Partnership Agreement (SPA), signé le 17 juillet 2018.

¹⁰²⁰ Personal Information Protection Commission, "Amendment to the Act on the Protection of Personal Information," September 2018.

¹⁰²¹ Cour Suprême du Japon, arrêt du 4 juillet 2018, affaire n° 17.

Pour la Commission, un accord PNR entre l'UE et le Japon « contribuerait à renforcer le partenariat » entre Européens et Japonais pour « une connectivité durable et des infrastructures de qualité », parmi lesquelles la sécurité du transport aérien. Ces réflexions sont survenues dans un contexte de développement des échanges de données. En effet, le 23 janvier 2019, la Commission européenne a adopté une décision d'adéquation relative à l'accord de transfert de données à caractère personnel, entre opérateurs commerciaux, vers le Japon¹⁰²². La Commission a veillé à évaluer les conditions et les garanties attachées à l'accès des pouvoirs publics japonais, notamment les services répressifs, aux données à caractère personnel traitées par les opérateurs concernés.

Lors de sa préparation pour la réception des Jeux olympiques de 2020, le Japon a fait de la transmission des données des dossiers passagers par les transporteurs venant de l'Union européenne un impératif afin de pouvoir faire face à la hausse prévue des risques en termes de sécurité¹⁰²³. C'est dans ce contexte que le Japon a formellement exprimé à la Commission européenne son souhait d'engager des négociations dans l'intention de conclure un accord PNR avec l'Union européenne¹⁰²⁴.

Le 27 septembre 2019, le Conseil a ainsi recommandé à la Commission d'engager des négociations avec le Japon en vue de la signature d'un accord bilatéral définissant le cadre et les conditions dans lesquels les transporteurs aériens seraient autorisés à transférer les données des dossiers passagers au Japon, tout en garantissant le respect des exigences du droit de l'Union européenne¹⁰²⁵. L'annexe de la recommandation a ensuite établi les directives de négociation du Conseil à l'intention de la Commission, autrement dit les objectifs que celle-ci devait viser au nom de l'Union européenne au cours des négociations.

Cette recommandation a été adoptée conformément à la procédure prévue à l'article 218 du TFUE relative aux accords conclus entre l'Union et les pays tiers¹⁰²⁶. À travers ce document,

¹⁰²² Commission, Décision d'exécution (UE) 2019/419 de la Commission du 23 janvier 2019 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Japon en vertu de la loi sur la protection des informations à caractère personnel.

¹⁰²³ Commission européenne, Recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et le Japon aux fins du transfert et de l'utilisation de données des dossiers passagers (PNR) afin de prévenir et de combattre le terrorisme et d'autres formes graves de criminalité transnationale, 27 septembre 2019.

¹⁰²⁴ Ibidem.

¹⁰²⁵ Commission européenne, Recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et le Japon aux fins du transfert et de l'utilisation de données des dossiers passagers (PNR) afin de prévenir et de combattre le terrorisme et d'autres formes graves de criminalité transnationale, COM(2019) 420 final, Bruxelles, 27 septembre 2019.

¹⁰²⁶ CEPD, Avis 3/2019 relatif à la participation aux négociations en vue d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité, 2 avril 2019.

la Commission a aspiré à obtenir du Conseil l'autorisation de négocier, au nom de l'Union, et à engager des négociations avec le Japon, conformément au mandat de négociation. Le Parlement européen devra approuver le texte de l'accord, une fois les négociations terminées, puis le Conseil adoptera une décision ouvrant la voie à la conclusion formelle de l'accord.

Le CEPD a été amené à donner son avis dans un contexte où les accords PNR n'étaient pas encore solidement ancrés dans le paysage juridique international. En effet, en 2011, seuls deux accords internationaux relatifs au traitement et au transfert des données PNR avaient été conclus entre l'Union européenne et des pays tiers, l'un avec les États-Unis et l'autre avec l'Australie. Après un arrêt de la Cour de justice, celui conclu avec le Canada, nous l'avons vu, a pris la voie de nouvelles négociations en juin 2019 pour pouvoir se mettre en conformité avec les conditions énoncées par la Cour.

Sur le plan européen, le CEPD a dû, cette fois-ci, tenir compte dans la définition du cadre juridique sur le traitement de données des dossiers passagers des nouvelles dispositions de la directive européenne relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, adoptée le 27 avril 2016.

Le CEPD a formulé un certain nombre de recommandations visant à améliorer les directives de négociation entre les autorités européennes et japonaises. Premièrement, au regard du principe de nécessité et de proportionnalité, il a considéré que l'un des objectifs des négociations devrait permettre d'assurer que l'accord euro-japonais comporte les garanties matérielles et procédurales nécessaires, permettant de garantir la proportionnalité du système PNR. Le Contrôleur européen plaida ainsi pour une approche stricte quant à la nécessité et à la proportionnalité du système.

Deuxièmement, conformément au principe de limitation de la finalité, le CEPD a recommandé que toute utilisation ultérieure des données des dossiers passagers transférées à d'autres fins devrait être dûment justifiée, définie d'une manière précise, claire et limitée à ce qui est strictement nécessaire.

Troisièmement, dès lors que l'accord envisagé entre dans le périmètre des objectifs suivis par l'article 16 TFUE, à savoir le droit à la protection des données à caractère personnel¹⁰²⁷, le CEPD recommanda que la décision du Conseil autorisant l'ouverture de négociations

¹⁰²⁷ E. THELISSON, « La portée du caractère extraterritorial du Règlement sur la protection des données », *Revue internationale de droit économique*, Association internationale de droit économique, pp. 501-533, en ligne à URL : <https://www.cairn.info/revue-internationale-de-droit-economique-2019-4-page-501.htm> consulté le 13 novembre 2023.

contienne une référence non seulement de la base juridique procédurale, mais également de la base juridique matérielle, comprenant ainsi l'article mentionné.

Quatrièmement, l'autorité européenne a fait observer que les négociations doivent accorder un intérêt particulier à la prévention du risque de divulgation indirecte de catégories particulières de données relatives aux passagers aériens ainsi qu'à la prévention du risque de réidentification des personnes physiques après l'anonymisation des données PNR qui les concernent¹⁰²⁸.

Cinquièmement, l'accord envisagé devrait renfermer des clauses permettant de le suspendre en cas d'infraction aux règles qui sont prévues et de le résilier dans le cas où les manquements sont graves et persistants¹⁰²⁹.

Sixièmement, l'organe indépendant a recommandé de préciser, dans les directives de négociation, si la coopération policière et judiciaire envisagée entre les autorités policières et judiciaires des États membres européens et les autorités publiques compétentes japonaises, ainsi qu'avec Europol et Eurojust, engloberait de tels transferts de données opérationnelles à caractère personnel de l'Union européenne vers le Japon. Si tel était le cas, le CEPD préconise d'inclure, au minimum, des références à la base juridique appropriée pour les transferts de données opérationnelles à caractère personnel.

Septièmement, le CEPD recommanda d'identifier clairement les autorités spécifiques japonaises qui seront chargées de la surveillance indépendante du respect des règles prévues par l'accord PNR¹⁰³⁰.

Huitièmement, le CEPD encouragea les parties à développer la coopération internationale en matière de protection des données à caractère personnel dans le domaine des données des dossiers passagers.

Neuvièmement, l'organe européen invita la Commission à garantir, dans le futur accord, que les « données à caractère personnel anonymes » soit clairement définies dans l'accord comme étant des données personnelles anonymes et qu'en conséquence la personne concernée ne sera plus identifiable.

¹⁰²⁸ CEPD, Avis 6/2019 sur le mandat de négociation d'un accord entre l'UE et le Japon pour le transfert et l'utilisation de données des dossiers passagers, 25 octobre 2019. Lire aussi. P. GOSSELIN, « Les libertés individuelles et collectives à l'heure du numérique et de l'état d'urgence sanitaire », Gouverner à l'ère numérique, *L'ENA hors les murs*, 2020, pp. 10-12.

¹⁰²⁹ Ibidem.

¹⁰³⁰ Ibid.

Dixièmement, le CEPD recommande à la Commission d'accorder un intérêt spécifique à la définition des catégories de données PNR aux fins de l'accord, dans le but d'empêcher la possibilité de traiter et de transférer des informations susceptibles de révéler indirectement des catégories particulières de données relatives aux passagers aériens, telles que les convictions religieuses ou philosophiques ou les données relatives à la santé¹⁰³¹.

Par cet avis, le CEPD a réaffirmé sa mission de conseiller les institutions de l'Union européenne sur l'application logique et cohérente de l'arsenal de protection des données de l'Union européenne lors de la négociation d'accords dans le secteur répressif, conformément à l'action n° 5 de la stratégie du CEPD qui prévoit d'« intégrer la protection des données dans les politiques internationales »¹⁰³². Cet avis s'est fondé sur une obligation générale qui exige que les accords internationaux conclus par l'UE soient conformes aux dispositions du TFUE et respectent les droits fondamentaux formant le cœur du droit européen. Les acteurs du droit européen tentent de veiller à ce que l'article 8 de la Charte des droits fondamentaux de l'Union européenne, ainsi que l'article 16 du TFUE, soient respectés dans le cadre européen¹⁰³³.

Ainsi, en février 2020, le Conseil a adopté une décision autorisant l'ouverture de négociations entre l'Union européenne et le Japon en vue d'un accord sur le transfert et l'utilisation de données des dossiers passagers afin de prévenir et de combattre le terrorisme et d'autres formes graves de criminalité transnationale. Cette décision a permis à la Commission d'entamer des négociations avec le Japon, à la lumière des directives de négociation adoptées par le Conseil.

¹⁰³¹ Ibid.

¹⁰³² CEPD, « La stratégie du CEPD 2015-2019 », 2015, en ligne à URL : https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_fr.pdf consulté le 13 novembre 2023.

¹⁰³³ CEPD, Avis 6/2019 sur le mandat de négociation d'un accord entre l'UE et le Japon pour le transfert et l'utilisation de données des dossiers passagers, 25 octobre 2019.

Conclusion de la première partie

Cette première partie a mis en évidence la prééminence des législations répressives dans le traitement, l'utilisation et le transfert des données des dossiers passagers, révélant un conflit entre les exigences de sécurité collective et la protection des droits fondamentaux. D'un côté, le droit américain impose des obligations strictes en matière de transmission des données pour des raisons de sécurité nationale, ce qui est en contradiction avec le droit européen, qui défend la vie privée et la protection des données personnelles. Paradoxalement, bien qu'il y ait un consensus sur l'objectif de sécurité des échanges de données des passagers aériens, comme le montre l'accord euro-américain et la directive européenne, cette approche entraîne une atteinte significative aux droits fondamentaux des passagers. Les accords PNR révèlent une absence d'une protection juridique effective, avec une restriction notable des droits individuels au nom de la sécurité collective. Bien que les institutions européennes, telles que le Conseil et la Commission, privilégient des mesures sécuritaires, elles ne garantissent pas toujours une protection équilibrée des droits fondamentaux. En revanche, le Parlement européen, la Cour de justice, le Comité européen de la protection des données et le Contrôleur européen de la protection des données s'efforcent de maintenir un équilibre délicat entre sécurité et libertés individuelles.

PARTIE II – LES NOUVELLES MENACES SUR LA PROTECTION JURIDIQUE DES DOSSIERS PASSAGERS

La protection des données personnelles se trouvent confrontées à de nouveaux défis en raison de la mondialisation et du développement de la technologie qui a généré la collecte et le partage de données personnelles à grande échelle de manière très peu régulée¹⁰³⁴. Les entreprises comme les pouvoirs publics, peuvent utiliser des données personnelles dans le cadre de leurs activités, ce d'autant plus facilement que les personnes, à travers le monde, fournissent de plus en plus facilement des données à caractère personnel¹⁰³⁵ sur elles-mêmes. Aussi, les données à caractère personnel circulent librement à travers le monde¹⁰³⁶, par la prouesse des technologies, transformant les relations économiques et sociales. L'Union européenne est également concernée par ce phénomène puisque les données à caractère personnels de ses citoyens sont transférées vers des pays tiers et des organisations internationales.

Or, de telles transformations requièrent l'adoption d'un cadre juridique assurant la protection des données et des droits fondamentaux des citoyens européens¹⁰³⁷. La question de la garantie d'un niveau élevé de protection des données à caractère personnel est régulièrement discutée. En effet, il semble important de mettre en place un cadre qui maintiendra la confiance des citoyens, indispensable pour le développement de l'économie numérique sur le marché européen. Face aux impacts de ces transformations sur leurs droits fondamentaux, les personnes physiques aspirent à garder le contrôle de leurs données à caractère personnel. La sécurité pratique et juridique doit être renforcée à la fois pour les individus, les autorités publiques et les opérateurs économiques.

L'intégration économique et sociale résultant de la mise en place du marché intérieur européen a conduit à une substantielle augmentation des flux transfrontaliers de données à

¹⁰³⁴ L. OBADIA, « Technologies mondialisées, mondialisation technologique, Digital Globalization : quels liens entre les NTIC et la mondialisation ? », *Diogène*, vol. 271-272, n° 3-4, 2020, pp. 110-132.

¹⁰³⁵ F. NWAMEN, « Impact des technologies de l'information et de la communication sur la performance commerciale des entreprises », *La Revue des Sciences de Gestion*, vol. 218, n° 2, 2006, pp. 111-121.

¹⁰³⁶ B. JUANALS, « Protection des données personnelles et TIC au cœur des enjeux de société et de la mondialisation : les mécanismes d'un contrôle distribué », *tic&société*, vol. 8, n° 1-2, 1^{er} semestre 2014 et 2^e semestre 2014, en ligne à URL : <http://journals.openedition.org/ticetsociete/1475> consulté le 19 novembre 2023.

¹⁰³⁷ S.RODOTA, « Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives », *Mouvements*, vol. 62, n° 2, 2010, pp. 55-70.

caractère personnel, dont ceux des passagers aériens¹⁰³⁸. Les échanges de données à caractère personnel entre différents acteurs se sont intensifiés dans le monde. Le droit européen exige que les autorités nationales des États membres coopèrent et échangent des données personnelles pour accomplir leurs missions ou exécuter des tâches au nom d'une autre autorité d'un État membre¹⁰³⁹.

La politique de gestion des frontières des pays européens notamment a dû s'adapter à des évolutions considérables, du siècle dernier à notre dernière décennie, comme l'arrivée sans précédent de réfugiés et de migrants en situation irrégulière, la pandémie de Covid-19 et la guerre en Ukraine. Le renforcement des préoccupations en matière de sécurité de la part des services étatiques et l'introduction d'acteurs privés dans le domaine de la protection des frontières ont une incidence sur la protection juridique des dossiers passagers (Titre 1).

Face à ces menaces, l'Union européenne et ses États membres ont mis en œuvre des mesures concrètes dans le but de préserver la sécurité de l'Europe et de renforcer ses frontières extérieures dont l'établissement de l'Agence européenne de garde-frontières et de garde-côtes Système d'information Schengen, un système d'information sur les visas, des vérifications systématiques, un système d'entrée/de sortie, un système en ligne pour l'autorisation des voyages, un contrôle temporaire aux frontières intérieures et une interopérabilité des bases de données¹⁰⁴⁰. Cette dernière mesure vise à régler le problème de la fragmentation des systèmes d'information au sein de l'Union européenne qui cause un déficit informatif. En effet, les systèmes d'information de l'Union utilisés par les autorités pour contrôler les frontières, gérer les flux migratoires et lutter contre la criminalité, ne sont pas interconnectés.

En mai 2019, le Conseil a adopté deux règlements qui visaient à établir un cadre pour l'interopérabilité des systèmes d'information de l'Union afin d'améliorer la gestion des frontières, de la migration et de la sécurité¹⁰⁴¹. Ce système d'interopérabilité a mis en place les éléments suivants : un portail de recherche européen qui permet aux autorités compétentes d'effectuer des recherches en parallèle dans de multiples systèmes, en utilisant des données

¹⁰³⁸ 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).

¹⁰³⁹ Ibidem.

¹⁰⁴⁰ Europa, « Renforcer les frontières extérieures de l'UE », en ligne à URL : <https://www.consilium.europa.eu/fr/policies/strengthening-external-borders/> consulté le 5 janvier 2023.

¹⁰⁴¹ Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 concernant l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice (eu-LISA) et modifiant le règlement (UE) 1077/2011. Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 relatif à l'interopérabilité des systèmes d'information de l'Union européenne dans le domaine de la liberté, de la sécurité et de la justice.

biométriques et biographiques, un service partagé de mise en correspondance de données biométriques permettant de rechercher et de comparer les données biométriques comme les empreintes digitales et images faciales issues de nombreux systèmes, un répertoire commun de données d'identité qui devrait regrouper les données biographiques et biométriques des ressortissants de pays tiers disponibles dans plusieurs systèmes d'information de l'Union et un détecteur d'identités multiples chargé de vérifier si les données d'identité biographiques provenant de la recherche existent dans d'autres systèmes couverts, afin de permettre de détecter les identités multiples liées au même ensemble de données biométriques¹⁰⁴².

Depuis les attentats du 11 septembre 2001 et sous l'impulsion des États-Unis, l'utilisation des données personnelles des passagers aériens, données PNR, s'est imposée. Les attentats en France (2015) et en Belgique (2016) n'ont fait qu'accélérer ce mouvement visant à leur utilisation de manière plus accrue. Au sein de l'Union européenne, la directive PNR a été adoptée, le 27 avril 2016, pour être appliquée dès le 25 mai 2018. Dans ce contexte, les échanges de données personnelles de passagers aériens multiplient le fichage aux frontières sans faire l'unanimité. Pour Xavier Latour, en raison de son ampleur, cette collecte massive de données personnelles relève d'une surveillance généralisée et d'une ingérence dans la sphère privée des passagers¹⁰⁴³.

Une autre menace se profile pour la protection juridique des dossiers passagers ; elle touche le territoire, comme un substrat de la localisation des activités humaines, qui est dépassé en l'état actuel des mouvements des personnes, des capitaux et des objets. La déterritorialisation vue comme l'effacement de l'État territorial devant les flux transnationaux signifie l'affaiblissement de contrôles d'accessibilité, des frontières internationales, et donc des contraintes spatiales imposées par les États et autres formes de gouvernement¹⁰⁴⁴. Cette évolution a pour conséquence un affaiblissement de la protection juridique des dossiers passagers puisque les droits nationaux, comme communautaires, sont dépassés, ces derniers n'étant plus capables de régir des flux supranationaux (Titre 2). En effet, des risques importants pèsent sur la protection des personnes physiques, en particulier en ce qui concerne les données des voyageurs européens. Les différences dans les standards de protection des droits et libertés des personnes physiques, en particulier le droit à la protection des données

¹⁰⁴² Conseil de l'UE, Communiqué de presse, « Interopérabilité des systèmes d'information de l'UE: le Conseil adopte des règlements », *Europa*, 14 mai 2019, en ligne à URL : <https://www.consilium.europa.eu/fr/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/> consulté en ligne le 5 janvier 2022.

¹⁰⁴³ X. LATOUR, « Les fichiers PNR et les transports aériens internationaux », *Annuaire du droit de la sécurité et de la défense* 2018, Mare et Martin, 2018, pp. 247-258.

¹⁰⁴⁴ B. BADIE, *La fin des territoires*, Fayard, 1995.

personnelles, à l'égard du traitement des données à caractère personnel dans les États membres, peuvent créer un obstacle au libre flux desdites données dans l'ensemble de l'espace communautaire¹⁰⁴⁵. Ces différences peuvent dès lors constituer un obstacle à l'exercice des activités économiques, fausser la concurrence et empêcher les principaux acteurs européens de s'acquitter des obligations qui leur incombent en vertu du droit européen¹⁰⁴⁶.

Le territoire est une notion centrale dans toute organisation humaine, où l'homme, plus tard le citoyen, cherche à fixer un territoire afin de garantir son existence et la perpétuation de son groupe. Élément constitutif de l'État, le territoire est considéré comme une condition déterminante de son existence, les États-nations se définissant ainsi essentiellement par l'existence de leur territoire¹⁰⁴⁷. Cette notion de territoire demeure indissociable de l'exercice de la souveraineté. Dans le cadre de l'exercice de ses prérogatives régaliennes, l'État est appelé à mobiliser des moyens, *a priori* publics, pour gérer les mouvements de populations. L'entrée et la sortie dudit territoire de l'État relève de l'exercice de sa souveraineté.

En droit de la sécurité sociale, le droit dérivé a admis la déterritorialisation des règles de sécurité sociale nationales et a fait de l'Union européenne l'espace d'application de chaque droit national¹⁰⁴⁸. Cette législation vise à faire que chaque loi nationale soit rendue applicable hors de son territoire. Ici, l'internationalisation des législations est devenue nécessaire pour protéger la protection sociale du migrant. Elle passait par la déterritorialisation de leurs conditions.

En droit de la protection des données personnelles, une réflexion reprenant la même dialectique semble nécessaire, car la déterritorialisation affaiblit la protection des passagers aériens. Une réponse à l'échelle supranationale paraît alors être l'une des solutions à adopter pour que la protection juridique des dossiers passagers soit effective.

¹⁰⁴⁵ 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).

¹⁰⁴⁶ Ibidem.

¹⁰⁴⁷ J-M PONTIER, « Territorialisation et déterritorialisation de l'action publique », *L'Actualité juridique*, Droit administratif, 1997.

¹⁰⁴⁸ P. RODIÈRE, « Sécurité sociale - Droit de l'Union européenne », *Répertoire de droit international*, Dalloz, avril 2019.

TITRE 1 – L’AFFAIBLISSEMENT DE LA PROTECTION JURIDIQUE DES DOSSIERS PASSAGERS DANS LEUR TRAITEMENT AUX FRONTIÈRES

La gestion des frontières est devenue une priorité pour les États membres de l’Union européenne en raison de la pression migratoire et de la vague des attentats qui a touché les États européens depuis le début du siècle. Une modernisation de la gestion des frontières extérieures a été initiée avec la mise en place d’une base de données commune visant à renforcer la sécurité des citoyens européens et de lutter contre le terrorisme et les formes graves de criminalité. Cette volonté repose sur le concept de « frontières intelligentes » (Smart Borders)¹⁰⁴⁹ selon lequel l’Union européenne, à travers le Parlement européen, a pris des mesures depuis 2013. Elle détient à présent un arsenal ambitieux qui passe par l’identification de manière systématique des personnes qui entrent dans l’espace Schengen. Or, le contrôle des visiteurs, la collecte massive de données et la création de registres, tels que les dossiers passagers, n’est pas sans conséquence ; il existe un risque d’affaiblissement de la protection juridique des dossiers passagers dans la gestion du contrôle des frontières (Chapitre 1) sachant que ce type de système stocke des informations accessibles aux autorités frontalières et à mises à disposition aux fins d’enquêtes. Avec un nombre de visiteurs en croissance, on parle de 887 millions¹⁰⁵⁰ visiteurs dans l’espace Schengen en 2025, le nombre de données recueillies représente une masse non négligeable¹⁰⁵¹.

Le système PNR permet aux services répressifs postés aux frontières de prévenir et de détecter des infractions graves comme terrorisme, à enquêter sur celles-ci et à poursuivre leurs auteurs. Lorsque cela est fait en temps réel, les données PNR permettent d’identifier des personnes non-soupçonnées de participation à une infraction grave ou à un acte de terrorisme mais dont l’analyse des données indique qu’elles peuvent être impliquées dans une infraction de cette nature et qu’elles devraient donc être soumises à un examen approfondi par les autorités compétentes. Ce système leur permet également d’identifier les personnes dont les

¹⁰⁴⁹ S. RODRIGUES, « Transports aériens », *Répertoire de droit européen*, Dalloz, 2018.

¹⁰⁵⁰ Thales, « Le système électronique d’Entrée-Sortie en zone Schengen: la biométrie au service des frontières intelligentes », en ligne à URL : <https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/biometrie/systeme-entree-sortie> consulté le 15 janvier 2024.

¹⁰⁵¹ Ministère de l’Intérieur, « En 2025, l’Union européenne déploie de nouveaux outils dédiés aux voyageurs étrangers pour sécuriser son territoire », 19 septembre 2023, en ligne à URL : <https://www.interieur.gouv.fr/actualites/actualites-du-ministere/en-2025-lunion-europeenne-deploie-de-nouveaux-outils-dedies-aux> consulté le 19 novembre 2023.

données de déplacement sont suspectes, comme les ressortissants européens soupçonnés de vouloir rejoindre les mouvements djihadistes en Afrique, au Proche Orient ou en Asie centrale¹⁰⁵².

Les données PNR peuvent être perçues comme un instrument de contrôle aux frontières. Cette collecte massive et le profilage qui en découle peuvent être considérés comme un mécanisme intrusif car ils impliquent la collecte et l'utilisation à court, moyen ou long terme de toutes les informations touchant au passager aérien. L'intrusion peut se caractériser par le nombre de catégories de données qui sont utilisées – elles sont au nombre de dix-neuf – pour un accord PNR standard. En effet, cette technique aboutit à nier l'essence même de l'Homme en le réduisant à une catégorie sur la base de calculs statistiques, sans avoir égard à sa possibilité de changer.

L'individu peut être ainsi réduit à une prédiction comportementale. En criminologie, le profilage désigne « l'établissement du profil psychologique de l'individu recherché » sachant que la personnalité est classiquement définie comme « la synthèse des éléments constituant la situation mentale et psychologique de l'individu »¹⁰⁵³. La moindre donnée personnelle est considérée comme étant susceptible de renseigner sur les agissements futurs de l'individu qu'elles concernent. Néanmoins, le préalable est de valider le degré de prédictibilité de la donnée étudiée et ce n'est que si la valeur prédictive est élevée que la prise en compte des prévisions peut être considérée comme pertinente.

Le profilage ethnique quant à lui va à l'encontre du principe d'égalité de tous devant la loi et le droit de chacun à un traitement égal. Cette technique peut ainsi être assimilée à une forme de discrimination raciale, interdite par le droit international. Dans le cadre européen, elle remet en cause l'engagement de faire de la non-discrimination l'une des valeurs fondamentales de l'Union européenne. De plus, le profilage ethnique est inefficace, voire contre-productif, car il stigmatise des communautés dont précisément la coopération est nécessaire pour lutter contre la criminalité transnationale et le terrorisme¹⁰⁵⁴.

Or, les politiques actuelles, comme le système PNR l'atteste, s'en remettent de plus en plus aux données à caractère personnel pour anticiper les comportements individuels¹⁰⁵⁵. En effet,

¹⁰⁵² P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

¹⁰⁵³ J. EYNARD, « Quelle définition pour un régime de protection efficace ? », *Les données personnelles*, Michalon, pp. 109-132, 2013.

¹⁰⁵⁴ Ibidem

¹⁰⁵⁵ J. LAGASSE, « 'Fichier' PNR : surveillance électronique de masse ou nouveau paradigme de la sécurité ? », *Les Notes du CREOGN*, 2016.

ces nouvelles techniques permettent de suivre, quasiment en temps réel, les individus dans leurs déplacements, ce qui est nécessaire pour détecter ceux qui pourraient présenter des risques d'atteintes aux personnes et aux biens¹⁰⁵⁶. Toutefois, les critiques insistent en particulier sur l'insuffisance d'éléments d'information et de retours d'expérience démontrant l'utilité et la nécessité de la collecte de données des passagers aériens à des fins répressives. Ainsi, le G29 et le Contrôleur européen de la protection des données remarquent l'absence d'éléments chiffrés démontrant l'utilité et la nécessité de ces données pour les services de sécurité¹⁰⁵⁷.

Aujourd'hui, on observe de nouvelles dynamiques qui, conjuguées, peuvent produire de nouvelles formes de profilage racial. Dans le même temps, l'Europe est confrontée à de nouvelles menaces terroristes avec la possibilité d'attentats dirigés par certains groupes djihadistes et l'émergence d'un « terrorisme local » qui trouve son inspiration dans ces groupes¹⁰⁵⁸. Les profils des criminels européens qui ont commis les attentats terroristes ayant touché l'Europe ces dernières années, notamment la France, ressemblent aux personnages des romans de Dostoïevski : Stavroguine, Kirillov, Chatov, Verkhovenski ou Chigalev. Aujourd'hui, les terroristes djihadistes sont d'origine pakistanaise ou tchéchène et ils représentent une seconde génération dont les pères et mères ont quitté un territoire en guerre ou instable. La France de 2015 n'est pas la Russie de 1855¹⁰⁵⁹ mais leur jeunesse se ressemblent et tous ont en commun le déracinement. Pendant ce temps, le rejet de l'immigration est en augmentation à travers l'Europe, accompagné de campagnes ciblant les immigrés. Ces évolutions ont pour conséquence une augmentation du profilage religieux et racial. En effet, ces techniques sont vues comme un moyen de concentrer plus efficacement les ressources en matière d'application de la loi et de renseignement, de repérer les potentiels terroristes et d'arrêter les immigrants illégaux.

La participation de personnes privées au contrôle des migrations en Europe, en France notamment, est devenue au fil des années une réalité visible pour tout utilisateur des transports aériens. Bien que la maîtrise des frontières soit l'une des principales missions de l'État, aujourd'hui, s'il continue de contrôler les mouvements de populations, force est de constater qu'il n'exerce plus seul cette prérogative. De différentes façons, des personnes

¹⁰⁵⁶ J. EYNARD, « Quelle définition pour un régime de protection efficace ? », *Les données personnelles*, Michalon, pp. 109-132, 2013.

¹⁰⁵⁷ S. SUTOUR, Y. DETRAIGNE, « Rapport n° 401 : La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives », Commission des lois, Sénat, 13 mai 2009

¹⁰⁵⁸ O. ROY, *Le djihad et la mort*, Editions Seuil, 2016, p. 50

¹⁰⁵⁹ G. FERRAGU, « L'invention du mythe terroriste : la Russie et ses Démons », *Histoire du Terrorisme*, 2014, pp. 61-95.

privées, professionnels de la sécurité ou transporteurs, interviennent de plus en plus aux côtés des acteurs étatiques.

Bien que justifiée, car les moyens humains et matériels de l'État ne peuvent plus répondre aux besoins de surveillance que requiert la croissance des mouvements migratoires, l'extension d'une délégation publique aux acteurs privés en matière de contrôle des frontières peut contribuer à l'affaiblissement de la protection des données des passagers (Chapitre 2).

Chapitre 1 – L’affaiblissement de la protection juridique des dossiers passagers par la collecte de données personnelles aux frontières

« Cicatrice laissée par l’histoire, la frontière intéresse le juriste. Elle contribue à permettre la distinction des droits nationaux, ainsi que la distinction du droit national et du droit international »¹⁰⁶⁰. C’est par cette phrase que le professeur François Terré introduit ses réflexions sur la problématique de la frontière (et du territoire) en droit. Si les frontières intéressent les juristes, c’est que la loi s’applique toujours à un moment donné et dans un espace particulier. Le philosophe Blaise Pascal avait commenté avec ironie la relativité spatiale du droit et sa tendance à se laisser enfermer dans des frontières : « Trois degrés d’élévation au pôle renversent toute la jurisprudence... Plaisante justice qu’une rivière borne ! Vérité au-deçà des Pyrénées, erreur au-delà »¹⁰⁶¹.

Les frontières et les législations sont parfois si étroitement liées qu’elles ne peuvent être considérées séparément mais leur relation demeure ambivalente. Jean-Jacques Rousseau, bien que partant d’une conception de l’état de nature diamétralement opposée à celle de Hobbes, attribuait aux frontières et aux bornes l’origine du droit : « Le premier qui, ayant enclos un terrain, s’avisa de dire: ceci est à moi, et trouva des gens assez simples pour le croire, fut le vrai fondateur de la société civile. Que de crimes, de guerres, de meurtres, que de misères et d’horreurs n’eût point épargnés au genre humain celui qui, arrachant les pieux ou comblant le fossé, eût crié à ses semblables: gardez-vous d’écouter cet imposteur; vous êtes perdus si vous oubliez que les fruits sont à tous, et que la Terre n’est à personne »¹⁰⁶². Si le droit définit des frontières, il les dépasse pour rendre la communication possible. Qu’il s’agisse de sa définition (frontières de lignes, de régions ou de groupes) ou de son dépassement (par le droit international public ou privé, l’immigration, la nationalité, les étrangers ou les compétences des travailleurs frontaliers), la notion de frontière ne cesse d’évoluer.

L’idée de frontière a une histoire très ancienne bien que ni chez les Grecs ni chez les Romains un concept bien évident ne semble avoir fait consensus. Le Moyen Âge, où dominait un système féodal au sein duquel se superposaient et s’enchêvêtraient les autorités politiques,

¹⁰⁶⁰ F. TERRE, *Introduction générale au droit*, Paris, Dalloz, 8^e éd. 2009, p. 426

¹⁰⁶¹ B. PASCAL, *Œuvres complètes*, II, Paris, Gallimard, Bibl. La Pléiade, 2000, « Pensées », fragment 56, p. 560

¹⁰⁶² J.-J. ROUSSEAU, *Discours sur l’origine et les fondements de l’inégalité parmi les hommes – Discours sur les sciences et les arts*, Partie II, Paris, Flammarion, 1995, p. 222

était moins propice à la notion jusqu'alors prédominante de frontière, qui suppose que les communautés communales soient géographiquement juxtaposées et juridiquement sur un pied d'égalité. Il faudra donc attendre l'émergence des grands et puissants États modernes, en passant de la suzeraineté à la souveraineté, pour voir l'apparition d'une acception plus précise des frontières¹⁰⁶³. Selon Charles Rousseau, le mot « frontière » serait ainsi apparu en France au XIV^e siècle avec les lettres de Louis X le Hutin du 30 novembre 1315 à propos de l'établissement et l'entretien des garnisons de Flandre¹⁰⁶⁴.

En tout état de cause, il existe aujourd'hui incontestablement une compréhension juridique de la frontière, à savoir la frontière territoriale qui délimite un espace de souveraineté. Il existe suffisamment d'éléments pour justifier l'actualité du sujet et la nécessité d'une réflexion juridique renouvelée. D'une part, il convient de noter qu'au moins 26 000 kilomètres de nouvelles frontières (parfois dans des zones instables) ont été établies depuis la « chute du mur »¹⁰⁶⁵. D'autre part, on relève certaines tentatives récentes de développer le concept juridique classique de frontières, notamment à des fins de contrôle. Enfin, la mondialisation des échanges et le progrès technologique ne peuvent qu'entraîner une évolution des règles juridiques dans les relations internationales, voire remettre en cause la pertinence même du concept de frontière territoriale.

Le développement des nouvelles technologies et de la technique en général a permis l'avènement d'une quantité incroyable de données. Ainsi, le *big data*¹⁰⁶⁶ renvoie à un gigantesque volume de données produites combiné à des capacités sans cesse accrues de stockage et à des outils d'analyse en temps réel de plus en plus sophistiqués. Cet état de fait offre aujourd'hui des possibilités inégalées d'exploitation des informations. Cela concerne naturellement le monde aérien et les frontières.

Recueillies et conservées par les transporteurs aériens, les données des dossiers passagers comportent différentes informations telles que le nom du passager, les dates du voyage, l'itinéraire, le numéro du siège, les données relatives aux bagages, les coordonnées du passager et le moyen de paiement utilisé. Cette collecte de données (section 1) s'inscrit dans un cadre juridique qui n'est pas insensible à cette opération puisque la directive PNR régit le transfert de ces données aux autorités répressives des États membres et leur traitement aux fins de la prévention et de la détection d'infractions terroristes ou de formes

¹⁰⁶³ C. BLUMANN, « Frontières et limites », in *La frontière*, Colloque de Poitiers, Paris, Pedone, 1980, p.4

¹⁰⁶⁴ C. ROUSSEAU, *Droit international public*, Paris, Sirey, 1977, tome III, p. 232

¹⁰⁶⁵ P. KLÖTGEN, *La frontière et le droit, esquisse d'une problématique*, Scientia Juris, 2011.

¹⁰⁶⁶ CNIL, « Big data », définition, en ligne à URL : <https://www.cnil.fr/fr/definition/big-data> consulté en ligne le 5 février 2022

graves de criminalité ainsi que des enquêtes et des poursuites en la matière. Une crainte existe cependant quant à un fait qui risque d'affaiblir les droits des passagers aériens : la surveillance généralisée des voyageurs par la collecte de masse de données.

Afin de protéger les droits fondamentaux en matière de protection des données à caractère personnel et le droit au respect de la vie privée, la directive PNR prévoit une série de restrictions en ce qui concerne le transfert, le traitement et la conservation des données des dossiers passagers. Semble ainsi consacré, par exemple, le principe selon lequel la collecte et l'utilisation de données sensibles est interdite. Par ailleurs, d'autres principes tentent de parer à l'affaiblissement de la protection des dossiers passagers comme la mise en place, requise de chaque État membre, d'une unité d'informations passagers chargée de la gestion et de la protection des données ; une unité qui doit comprendre un délégué à la protection des données et respecter l'obligation d'informer clairement les passagers aériens de la collecte de données PNR et de leurs droits à cet égard¹⁰⁶⁷.

Le profilage (section 2) est également encadré juridiquement, puisque le Conseil de l'Europe a rappelé que la collecte et le traitement de données sensibles des passagers dans le cadre d'un profilage sont interdits, sauf si ces données sont nécessaires et proportionnées aux finalités légitimes et spécifiques du traitement et pour autant que le droit national prévoit des garanties appropriées pour leur protection. De telles précautions sont nécessaires en raison du risque pour les droits et libertés des passagers aériens que le profilage porte dans la mesure où cette technique utilise les données personnelles d'un individu en vue d'analyser et de prédire son comportement, par exemple ses préférences ou ses habitudes de vie¹⁰⁶⁸.

Cette opération vise à évaluer certains des aspects personnels du passager aérien en vue d'émettre un jugement ou de tirer des conclusions sur lui¹⁰⁶⁹. Certaines de ces décisions sont entièrement automatisées, c'est-à-dire qu'elles ont été prises par le biais d'algorithmes appliqués aux données personnelles sans qu'aucun être humain n'intervienne dans le processus. Or, les décisions produites de manière automatique peuvent avoir des effets

¹⁰⁶⁷ V. GAUTRON, D. MONNIAUX, « De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme », *Archives de politique criminelle*, 2016, pp. 123-135.

¹⁰⁶⁸ T. HAMMARBERG, Commissaire aux droits de l'homme du Conseil de l'Europe, « Le profilage racial et religieux n'a pas sa place dans la lutte anti-terroriste », 29 mai 2007, en ligne à URL : http://www.coe.int/t/commissioner/Viewpoints/070529_fr.asp consulté le 19 novembre 2023.

¹⁰⁶⁹ K. DOUPLITZKY, « Le commerce de moi, modèle économique du profilage », in Traçabilité et réseaux, *Hermès La Revue*, 2009, pp. 113-117. Voir aussi A. MATTELART, A. VITALIS, « La captation et l'exploitation marchande des identités », *Le profilage des populations*, 2014, pp. 157-188.

négatifs sur les droits et les libertés d'un individu, notamment si elles entravent l'accès à un service ou un droit comme celui de se déplacer pour les passagers aériens¹⁰⁷⁰.

Section 1 – Une opération de collecte massive des données personnelles des passagers aériens

Polysémique, le terme de données revêt plusieurs sens. La donnée est associée à la recherche et la réflexion. Elle est le point de départ de la recherche, le pilier du raisonnement et du résultat. Dans le domaine de l'informatique, la donnée est définie comme la « représentation conventionnelle d'une information en vue de son traitement informatique »¹⁰⁷¹. Les données, informations produites numériquement, sont créées en permanence par les utilisateurs d'internet, les opérateurs et autres entités. Les données en lien avec chaque utilisateur sont les données personnelles que la CNIL définit comme « toute information identifiant directement ou indirectement une personne physique »¹⁰⁷². Pour les passagers aériens, des données comme le nom, l'itinéraire, les bagages, le moyen de paiement, l'itinéraire du déplacement, les vols concernés, le contact à terre du passager (numéro de téléphone), les tarifs accordés, l'état du paiement effectué, le numéro de carte bancaire du passager ou le numéro de siège permettent de mieux connaître les flux des passagers et de mieux tracer les flux aériens. L'utilisation de ces données PNR permet aux compagnies aériennes d'échanger des informations de réservation dans le cas où les passagers auraient besoin de vols de plusieurs compagnies aériennes pour atteindre leur destination.

La quantité des données concernant les passagers s'est accrue ces dernières années avec leur recueil systémique et à grande échelle. Les acteurs du secteur aéroportuaire ont aujourd'hui la capacité de traiter ces données massives, de transmettre et de livrer rapidement des informations autrefois difficiles d'accès, d'offrir des modèles prédictifs inédits et d'opérer des rapprochements inattendus. Le terme de *big data* est apparu dans la littérature scientifique au début des années 2000, notamment dans le secteur de la finance, au sujet du *trading* à « haute fréquence » dans le cas de traitement extrêmement rapide de millions et de milliards de transactions financières¹⁰⁷³. Au fil des années, les sources de données se sont multipliées. Ces données massives peuvent se recouper avec d'autres données qui d'habitude ne le sont pas et

¹⁰⁷⁰ D. RAMIREZ, J. HOOPEES, ET T. LAI QUINLAN, "Defining Racial Profiling in a PostSeptember 11 World", *American Criminal Law Review*, vol. 40, 2003, pp. 1195-1233.

¹⁰⁷¹ M. WOZNY, « Exploitation des données personnelles : raison commerciale, raison d'état et opportunités », *Mémoire*, Université de Lyon, août 2017.

¹⁰⁷² CNIL, « Définition données personnelles », Cnil en France, disponible à URL : <https://www.cnil.fr/fr/definition/donnee-personnelle> consulté en ligne le 3 avril 2023.

¹⁰⁷³ M. BERNELIN, S. DESMOULIN, T. LEFEVRE, « Données massives, big data et santé publique », *ADSP*, n° 112, 13 septembre 2020.

font l'objet de moyens d'analyses et de traitement, notamment à travers l'intelligence artificielle.

Le droit européen a élaboré un cadre pour appréhender ce phénomène de collecte massive de données personnelles (sous-section 1) qui vise notamment à protéger la vie privée des individus et à réglementer la collecte et le traitement des données personnelles, y compris en cas de collecte massive de données. Les entreprises opérant au sein de l'Union européenne sont tenues de respecter ces règles strictes, ce qui a eu un impact significatif sur la manière dont les données personnelles sont gérées et traitées, en particulier par les transporteurs aériens (sous-section 2). Le défi en la matière porte sur l'efficacité de ce cadre juridique que les acteurs européens ont mis en place.

Sous-section 1 – Le droit européen face à la collecte massive des données personnelles

Le droit dérivé de l'Union européenne consacre les droits à la protection des données personnelles et à la vie privée. Deux textes spécifient la manière dont les données peuvent être collectées et traitées. En premier lieu, le règlement européen 2016/679 sur la protection des données pose des règles générales et des droits concernant le traitement des données à caractère personnel¹⁰⁷⁴. Par ailleurs, la directive 2016/680, connue sous le nom de directive « Police – Justice », énonce des règles applicables au traitement des données à caractère personnel dans le cadre des opérations de répression à des fins de prévention et de détection des infractions pénales ainsi que d'enquêtes et de poursuites dans ce domaine¹⁰⁷⁵. Ces actes encadrent les grandes bases de données utilisées au sein de l'Union européenne pour la gestion des frontières telles que le système d'information sur les visas (VIS), le système d'entrée/sortie (EES) ou le système européen d'information et d'autorisation concernant les voyages (ETIAS), sachant que chaque dispositif dispose aussi d'un cadre spécifique pour la protection des données¹⁰⁷⁶. La directive PNR, quant à elle, a pour objet de réglementer le transfert par les compagnies aériennes des données passagers aux autorités nationales. Les

¹⁰⁷⁴ 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).

¹⁰⁷⁵ 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.

¹⁰⁷⁶ Agence des droits fondamentaux de l'Union européenne, « Guide pour la prévention du profilage illicite aujourd'hui et demain », 2019, en ligne à URL : https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_fr.pdf consulté le 28 juin 2023.

agences nationales peuvent alors confronter les données de passagers avec d'autres bases de données de personnes recherchées.

§ 1 – La collecte des données PNR dans les États membres avant la mise en place du cadre européen

Parallèlement au cadre européen d'harmonisation des législations sur la protection des données personnelles, certains États membres de l'UE avaient déjà mis en place des systèmes de collecte de données à grande échelle sur les passagers aériens.

Le Gouvernement britannique¹⁰⁷⁷ a, par exemple, lancé en 2004 un projet pilote intitulé « Semaphor »¹⁰⁷⁸. Ce projet visait à développer un système intégré pour la gestion des contrôles aux frontières, en utilisant notamment les données des dossiers passagers API (Advance Passenger Information) et PNR (Passenger Name Record)¹⁰⁷⁹. Ce programme fut suivi par *e-borders* qui incluait le transport maritime, ferroviaire et aérien. Ces données des passagers aériens ont été recueillies et analysées avant le voyage. Puis, à la frontière, les données biométriques des visas et des passeports ont également été utilisées. Enfin, un régime de facilitation reposant sur l'utilisation de la biométrie a été créé pour les passagers volontaires.

La mise en place du programme britannique a été progressive, l'objectif étant une installation complète en 2014. Au-delà de la lutte contre le terrorisme et le crime organisé, *e-borders* visait le contrôle aux frontières, la lutte contre l'immigration illégale et la fraude fiscale¹⁰⁸⁰. Contrairement aux données API qui sont collectées et traitées pour tous les modes de transports et pour tous les trajets, les données PNR ne sont collectées que pour certaines destinations, spécifiquement ciblées.

Selon les informations remises aux rapporteurs de l'Assemblée nationale française, 75% des flux de données de passagers concernaient alors le transport aérien, et étaient conservées pendant dix ans, dont cinq sur une base active et les cinq autres années sur une autre base,

¹⁰⁷⁷ À cette époque, le Royaume-Uni est encore membre de l'Union européenne. Le processus de sa sortie de l'Union, connu sous le nom de « Brexit », a été officiellement complété le 31 janvier 2020.

¹⁰⁷⁸ G. GEOFFROY, « Rapport d'information sur la proposition de directive relative à l'utilisation des données des dossiers 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 », *Commission des affaires européennes*, Assemblée nationale, 16 novembre 2011.

¹⁰⁷⁹ Le cadre européen d'harmonisation des législations en matière de données personnelles, en particulier la Directive 95/46/CE, était en place avant 2004. Ce cadre initial a été remplacé par le Règlement (UE) 2016/679, connu sous le nom de Règlement général sur la protection des données (RGPD), qui est entré en vigueur en mai 2018.

¹⁰⁸⁰ G. GEOFFROY, *op. cit.*

avec une possibilité d'accès au cas par cas¹⁰⁸¹. Ce programme aurait coûté 1,2 milliards de livres ; un montant qui a été jugé élevé par le rapporteur parlementaire compte tenu du « caractère extensif du programme » qui se caractérise par des finalités larges, plusieurs types de modes de transport et des déplacements internationaux, européens et nationaux. Outre des difficultés rencontrées lors de sa mise en œuvre initiale, le rapporteur a noté des surcoûts liés au caractère novateur du programme¹⁰⁸².

La collecte massive du programme *e-borders* concernait 330 millions de mouvements de passagers. Il en a résulté 89 000 arrestations. Toutefois, la collecte de données PNR était minoritaire dans le système britannique puisqu'elle ne concerna que 14 millions de données collectées chaque année¹⁰⁸³. Leur évaluation favorable du système par les autorités britanniques n'a pas été altérée par cette proportion minime, car le passage à un ciblage basé sur des critères prédéfinis plutôt que sur une intervention manuelle a considérablement renforcé l'efficacité des contrôles positifs. Mettant en avant l'efficacité de l'utilisation de ces données, le Gouvernement britannique a révélé qu'au cours d'un semestre en 2010, 212 kilos de cocaïne et 20 kilos d'héroïne avaient été saisis grâce à la collecte des données PNR¹⁰⁸⁴.

D'autres pays européens ont collecté les données PNR mais ce fut dans un cadre significativement moins développé que celui du Royaume-Uni. En 2009, le droit belge prévoyait, dans le cas d'une autorisation judiciaire donnée par le parquet, de demander aux compagnies aériennes d'obtenir un accès à leurs données PNR¹⁰⁸⁵. L'usage des données PNR pouvait être proactif ou réactif. Les autorités belges ont ainsi signalé que 95 % de l'ensemble des saisies de drogue réalisées en 2009 résultaient exclusivement ou essentiellement du traitement des données PNR¹⁰⁸⁶. Le droit suédois permettait aussi l'utilisation des données PNR dans le domaine du renseignement, de la lutte contre le terrorisme et les douanes. Les autorités suédoises ont déclaré que 65 à 75 % de l'ensemble des saisies de drogue effectuées sur leur territoire, en 2009, résultaient exclusivement ou essentiellement du traitement des données PNR¹⁰⁸⁷. Le droit danois permettait également l'utilisation des données PNR¹⁰⁸⁸.

¹⁰⁸¹ Ibidem

¹⁰⁸² Ibid.

¹⁰⁸³ Ibid.

¹⁰⁸⁴ Ibid.

¹⁰⁸⁵ En 2009, l'accès aux données PNR par les autorités judiciaires en Belgique était régi la loi sur la vie privée du 8 décembre 1992. Le 5 septembre 2018, la loi belge du 30 juillet 2018 sur la protection des personnes physiques en ce qui concerne le traitement des données personnelles a été publiée. Elle abroge la loi sur la vie privée du 8 décembre 1992 et intègre les principes du RGPD.

¹⁰⁸⁶ GEOFFROY, op. cit.

¹⁰⁸⁷ Ibidem. Le droit suédois avait légiféré après son entrée au sein de l'Union européenne en adoptant la législation Personal Data Act (Sw. personuppgiftslagen, SFS 1998:204) en 1998, se conformant ainsi à la Directive européenne 95/46/EC.

De son côté, la France avait d'abord créé, avec la loi du 18 décembre 2013, un programme propre qui a été utilisé, à titre expérimental, jusqu'au 31 décembre 2017¹⁰⁸⁹. Ce fichier « API-PNR France » était régi par les articles L. 232-7, R. 232-12 et suivants du Code de la sécurité intérieure (CSI). La loi n° 2017-1510 renforçant la sécurité intérieure et la lutte contre le terrorisme, du 30 octobre 2017, a pérennisé ce système tout comme un fichier propre au domaine maritime¹⁰⁹⁰. Prévu à l'article L. 232-7-1 du CSI, ce dernier, qui n'est lié à aucune initiative européenne, s'inspire du système PNR aérien sans que les données collectées soient identiques.

Dans un registre comparable, l'article L. 561-26 du Code monétaire et financier, issu de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, impose aux transporteurs routier¹⁰⁹¹, maritime, ferroviaire et aérien, ainsi qu'aux opérateurs de voyage de transmettre à TRACFIN¹⁰⁹², à sa demande, les informations relatives à l'identité, au déplacement et aux bagages des personnes transportées.

Nous notons que ces initiatives ne semblaient pas avoir pour priorité le respect d'un principe primordial des droits fondamentaux, à savoir celui de ne pas nuire. En effet, dans le passé, il y a eu des cas de mauvais usage de données collectées par des organismes nationaux de la statistiques ou d'autres types d'entités dont les conséquences en termes de respect des droits fondamentaux ont été extrêmement préjudiciables¹⁰⁹³. D'autres principes devraient également être pris au sérieux, notamment ceux qui concernent les mesures que doivent prendre les collecteurs de données afin de s'assurer que les informations relatives aux données personnelles, lorsqu'elles sont collectées à des fins statistiques raisonnables, ne soient pas

¹⁰⁸⁸ Ibid. Au Danemark, les deux législations Act on Processing of Personal Data du 1^{er} juillet 2000 et Data Retention Executive Order régissaient alors la collecte et la conservation des données à caractère personnel.

¹⁰⁸⁹ Délibération n° 2014-308 du 17 juillet 2014 portant avis sur un projet de décret relatif à la création d'un traitement de données à caractère personnel dénommé « système API-PNR France » pris pour l'application de l'article L. 232-7 du code de la sécurité intérieure et fixant les modalités de transmission au service à compétence nationale « Unité Information Passagers » des données relatives aux passagers par les transporteurs aériens. (demande d'avis n° 14014804)

¹⁰⁹⁰ Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

¹⁰⁹¹ Code monétaire et financier, article L. 561-26.

¹⁰⁹² Service de renseignement placé sous l'autorité du ministère de l'Économie, TRACFIN est une cellule de renseignement financier française qui a pour objectif de lutter contre les circuits financiers clandestins, le blanchiment de capitaux et le financement du terrorisme

¹⁰⁹³ C'est le cas de la plateforme Grindr, un site de rencontre qui a collecté et partagé les données sérologiques de ses membres, les rendant ainsi publiques. T. DOUVILLE, « Les dangers de la collecte des données de santé par les tiers intéressés (gafam, assureurs...) », *Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM)*, 20, 12-16, 2018. Lire également. S. PARASIE, « Des machines à scandale. Éléments pour une sociologie morale des bases de données », *Réseaux*, vol. 178-179, no. 2-3, 2013, pp. 127-161.

utilisées contre le consentement des personnes concernées et qu'elles soient conservées en lieux sûrs¹⁰⁹⁴.

Le droit à la vie privée est profondément lié aux questions touchant à l'identité personnelle et à l'autoidentification. Le Comité des droits de l'Homme des Nations-Unies a défini la vie privée comme la sphère de la vie d'une personne dans laquelle cette dernière peut librement exprimer son identité, que ce soit en nouant des relations avec d'autres ou en restant seule¹⁰⁹⁵. Par conséquent, les données à caractère personnel ne doivent pas être publiquement accessibles ou publiées d'une façon qui permet l'identification, directement ou indirectement, des personnes concernées.

Le respect des droits fondamentaux requiert une limitation au strict nécessaire des pouvoirs prévus par les différentes législations sur les données personnelles des passagers aériens. En l'espèce, le droit au respect de la vie privée et à la protection des données à caractère personnel, garanti en droit de l'Union européenne, ne doivent pas être sacrifiés au profit de la sécurité collective des citoyens.

§ 2 – La collecte des données PNR dans le cadre du droit de l'Union européenne

La collecte et le traitement de données personnelles ne sont pas nécessairement informatisés ; des fichiers papiers sont également concernés et doivent donc être protégés dans les mêmes conditions. Dans le cadre du droit européen, cette collecte doit être objective et doit poursuivre une finalité déterminée préalablement au recueil de ces données personnelles et à leur exploitation¹⁰⁹⁶. La collecte devient massive lorsqu'une multitude d'informations sur les individus sont agrégées et croisées, rendant l'identification des personnes physiques de plus en plus facile à réaliser¹⁰⁹⁷.

Devenue une opération classique dans les aéroports, la collecte de données personnelles est mise en œuvre par tous les transporteurs aériens pour les besoins de leurs activités¹⁰⁹⁸. Le

¹⁰⁹⁴ L'article 9 du RGPD interdit en principe le traitement des données sensibles, telles que celles révélant l'origine raciale, les opinions politiques, les croyances religieuses, ou les données de santé. Cependant, cette interdiction ne s'applique pas si le traitement est nécessaire à des fins d'intérêt public, de recherche scientifique ou historique, ou à des fins statistiques, à condition que ce traitement soit proportionné, respecte l'essence du droit à la protection des données, et soit encadré par des mesures spécifiques pour protéger les droits fondamentaux des personnes concernées.

¹⁰⁹⁵ Organisation des Nations-Unies, Comité des droits de l'Homme, *Coeriel and Aurik v the Netherlands* (1994), Communication n° 453/1991, par. 10.2

¹⁰⁹⁶ CNIL, « Traitement de données, définition », 2022.

¹⁰⁹⁷ C. CASTETS-RENARD, « La protection des données personnelles dans les relations internes à l'Union européenne, la protection des données personnelles en matière civile et commerciale », *Répertoire de droit européen*, Dalloz, novembre 2022.

¹⁰⁹⁸ S. PARIER, « L'action de groupe et le RGPD en matière de transport aérien », *Juris tourisme*, Dalloz, 2019, n° 215, p. 44.

passager aérien est amené, à tous les stades de son itinéraire, à confier ses précieuses données personnelles. L'itinéraire débute dès le stade de la réservation du billet où il doit renseigner son nom, son prénom et ses données bancaires¹⁰⁹⁹. L'opération se poursuit à l'aéroport de départ où le voyageur doit se plier à diverses opérations d'enregistrement et de contrôle de sécurité. Avant même de s'asseoir à son siège passager, le voyageur aura fait l'objet d'une collecte poussée de ses données à caractère personnel. Arrivé à destination, le voyageur devra encore se soumettre à divers dispositifs de collecte en passant par les formalités des douanes, de l'immigration et éventuellement de fouilles¹¹⁰⁰.

Dans le cadre du droit de l'Union européenne, la collecte massive de données personnelles, comme tout traitement de données, doit respecter le règlement général sur la protection des données personnelles (RGPD)¹¹⁰¹, qui constitue le cadre général européen en matière de protection de données à caractère personnel. De plus, la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) représente constitue un cadre juridique particulier à ce type de données¹¹⁰².

En principe, le responsable du traitement de données personnelles doit d'abord justifier l'opération qu'il entend appliquer sur l'une des bases légales prévues par le RGPD. Par ailleurs, le droit européen général rappelle que la collecte de données à caractère personnel doit être réduite à ce qui est strictement nécessaire au regard de la finalité poursuivie. Ce principe de minimisation prévoit que ces données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des buts pour lesquels elles sont traitées¹¹⁰³.

S'agissant de la protection juridique des dossiers passagers, le professeur Pascal Dupont considère que les 19 catégories de données personnelles de passagers aériens prévues par la directive PNR, qui permettent de tracer un passager aérien au cours de ses déplacements, ne concernent que les caractéristiques du vol sans avoir d'impact négatif sur la protection de la

¹⁰⁹⁹ Ibidem

¹¹⁰⁰ Ibid.

¹¹⁰¹ 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.

¹¹⁰² 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.

¹¹⁰³ RGPD, article 5. Cette disposition requiert que les données collectées soient être strictement limitées à ce qui est nécessaire pour atteindre l'objectif du traitement, évitant ainsi la collecte de données excessives ou non pertinentes.

vie privée. Pour lui, ces catégories ne constituent pas une collecte massive et indiscriminée de données personnelles¹¹⁰⁴.

L'article 13 de la directive en question introduit de nombreuses garanties visant à protéger le droit à la protection des données personnelles¹¹⁰⁵. Il prévoit que chaque État membre doit s'assurer que, pour tout traitement effectué en vertu de cette directive, chaque passager bénéficie du droit à la protection de ses données personnelles. Ce droit inclut l'accès, la rectification, l'effacement, et la limitation des données, ainsi que les droits à réparation et à un recours juridictionnel, conformément aux dispositions du droit de l'Union, du droit national, et aux articles 17, 18, 19 et 20 de la décision-cadre 2008/977/JAI¹¹⁰⁶. Cette décision cadre définit les concepts de données personnelles et de traitement associé, précisant que les autorités compétentes des États membres peuvent collecter des données à caractère personnel uniquement pour des finalités déterminées, explicites et licites¹¹⁰⁷. De plus, le traitement de ces données est strictement limité aux finalités pour lesquelles elles ont été initialement collectées¹¹⁰⁸.

En outre, les États membres disposent aujourd'hui d'unités d'information passagers (UIP), des autorités compétentes en matière de prévention et de détection des infractions terroristes, des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière. À défaut d'en disposer, l'État membre crée ou désigne une antenne d'une telle autorité. Sur le fondement de l'article 4 de la directive PNR, l'IUP est chargée « de la collecte des données PNR auprès des transporteurs aériens, de la conservation et du traitement de ces données, et du transfert de ces données ou du résultat de leur traitement aux autorités compétentes »¹¹⁰⁹. Ces unités jouent un rôle important dans la collecte massive de données, car elles sont chargées de procéder à l'évaluation du risque représenté par un passager, avant son arrivée ou son départ, pour identifier les personnes qui pourraient être en cause dans les infractions en lien avec le terrorisme ou le crime organisé et pour lesquelles un examen approfondi par les

¹¹⁰⁴ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

¹¹⁰⁵ Directive (UE) PNR, article 13.

¹¹⁰⁶ Décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

¹¹⁰⁷ 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.

¹¹⁰⁸ Directive (UE) PNR, article 13. Selon cette disposition, les données PNR doivent être utilisées uniquement aux fins spécifiques de prévention, de détection, d'enquête et de poursuites des infractions terroristes et des formes graves de criminalité.

¹¹⁰⁹ Directive (UE) PNR, article 4.

autorités compétentes est requis¹¹¹⁰. Ces unités peuvent être amenées à confronter les données PNR aux bases de données pertinentes, comme les bases de données internationales ou communautaires créées pour détecter les personnes et les objets recherchés ou visés par un signalement.

Le croisement de toutes ces données peut mettre à mal le principe de protection des données personnelles et de la vie privée des passagers aériens notamment s'il permet la détermination d'un risque à l'égard d'un passager en fonction, soit de son origine raciale ou ethnique, ses opinions politiques, ses convictions religieuses ou philosophiques, son appartenance à un syndicat, soit de données qui concernent sa santé ou sa vie sexuelle. Cependant, la directive a fait du délégué à la protection des données au sein de l'IUP le gardien de ce principe de protection puisque l'article 5 de la directive PNR rappelle qu'il est chargé « de contrôler le traitement des données PNR et de mettre en œuvre les garanties pertinentes »¹¹¹¹.

Cette volonté du législateur européen de répondre aux inquiétudes des individus n'a pas empêché certains chercheurs de considérer que les éléments contenus dans le fichier PNR européen ne suffisent pas à justifier la nécessité et la proportionnalité d'un système¹¹¹². À titre d'exemple, Xavier Latour considère que les données collectées sont alimentées par des éléments « trop largement appréciés » dans le fichier PNR européen, constituant ainsi une « ingérence excessive et susceptible de créer une suspicion abusive »¹¹¹³. Bien que l'Union européenne ait pris la décision d'interdire toute collecte d'information qui révèle de la race, la religion, l'ethnie ou les opinions politiques et syndicales, pour se recentrer sur les déplacements des passagers aériens, les données restent rassemblées lorsqu'elles arrivent chez les transporteurs et les opérateurs de voyage.

Cette masse de données collectée est transférée entre différents acteurs dans le domaine aérien national mais également international où il apparaît que les bénéficiaires américains, à titre d'exemple, vont au-delà de la seule administration des frontières. Ici, la frontière paraît trop poreuse, malgré le droit existant, notamment les accords et mesures portés par l'Union

¹¹¹⁰ G. GEOFFROY, « Rapport d'information sur la proposition de directive relative à l'utilisation des données des dossiers 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 », *Commission des affaires européennes*, Assemblée nationale, 16 novembre 2011.

¹¹¹¹ Article 5, *ibid.*

¹¹¹² G. GEOFFROY, « Rapport d'information sur la proposition de directive relative à l'utilisation des données des dossiers 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 », *Commission des affaires européennes*, Assemblée nationale, 16 novembre 2011.

¹¹¹³ X. LATOUR, « Les fichiers PNR et les transports aériens internationaux », *Annuaire du droit de la sécurité et de la défense 2018*, Mare et Martin, 2018, pp. 247-258.

européenne pour protéger les données personnelles des passagers aériens. À cet égard, X. Latour note que l'utilisation des données personnelles PNR dépasse « le strict contrôle aux frontières »¹¹¹⁴. Cet état de fait rendrait les objectifs poursuivis par le système PNR européen flous bien que le législateur les ait explicitement énumérés.

D'autres cas de collecte illicite de données à caractère personnel, par des entités étrangères ou des organismes publics européens dans l'espace européen, ont alerté les défenseurs de droits fondamentaux en Europe. Mentionnons notamment le scandale des écoutes de différentes personnalités européennes et mondiales dont des dirigeants politiques, des journalistes et des membres de la société civile permises par NSO, fabricant du logiciel espion israélien Pegasus¹¹¹⁵. Le logiciel permettait de réaliser des écoutes téléphoniques en donnant l'accès à des fichiers, des messages, des photos et d'autres applications sur le téléphone de la victime. Cet outil d'espionnage pouvait enregistrer des échanges, filmer une vidéo, permettre une géolocalisation à partir des appareils infectés même lorsqu'ils étaient éteints.

Officiellement, le logiciel Pegasus commercialisé par la société israélienne NSO et vendu qu'à des organismes gouvernementaux « ne collecte que les données provenant des appareils mobiles de personnes soupçonnées d'être impliquées dans des activités criminelles graves et terroristes »¹¹¹⁶. Cependant, un consortium de médias a révélé en 2023 que les cibles étaient beaucoup plus variées comme l'a révélé une enquête menée par une centaine de journalistes, coordonnée par Forbidden Stories avec le soutien technique du Security Lab d'Amnesty International, grâce à un accès exclusif aux coulisses de cet outil de surveillance commercialisé à de nombreux gouvernements en Asie, en Afrique, en Europe et en Amérique Latine. Parmi les victimes figurent des centaines de journalistes, de femmes et d'hommes politiques, de chefs d'entreprise du monde entier.

La violation de données a révélé un écart entre l'utilisation réelle du logiciel et les promesses de l'entreprise, qui a insisté dans son dernier rapport de transparence sur le fait que Pegasus n'est pas un outil de surveillance de masse et n'est utilisé que pour des raisons légitimes d'application de la loi ou de renseignement. Or, sur une période de deux ans, les enquêtes des journalistes ont montré que le seul client marocain avait sélectionné plus de 10 000 numéros

¹¹¹⁴ Ibidem

¹¹¹⁵ M. HENRY, « Après le scandale des écoutes, NSO, le fabricant du logiciel espion Pegasus, fait un grand ménage », *Le Figaro*, 21 août 2022, en ligne à URL : <https://www.lefigaro.fr/secteur/high-tech/depart-du-pdg-de-nso-fabricant-du-controverse-logiciel-espion-pegasus-20220821> consulté le 3 juillet 2023.

¹¹¹⁶ Forbidden Stories, « À Propos du Projet Pegasus », en ligne à URL : <https://forbiddenstories.org/fr/a-propos-du-pegasus-project/> consulté le 3 juillet 2023.

de téléphone pour une éventuelle surveillance¹¹¹⁷. Outre de nombreux abus sur les droits fondamentaux de citoyens, le logiciel Pegasus remet également en cause la stratégie globale de ces entreprises qui, tout en promettant de sélectionner des clients en fonction de leurs antécédents en matière de droits de l'Homme, a accepté de vendre sa technologie à des régimes non démocratiques tels que l'Azerbaïdjan, les Émirats Arabes Unis et l'Arabie Saoudite¹¹¹⁸.

La collecte de masse et illicite de données pose la question des mesures mises en place pour réguler l'utilisation d'armes de surveillance, tel Pegasus, et plus généralement de ces nouvelles techniques qui revendiquent de créer un monde meilleur et plus sûr. La dialectique sécuritaire de ces logiciels espions n'est pas sans rappeler la même que celle qui justifie la collecte des données personnelles des passagers aériens, dans le cadre des législations PNR, au nom de la lutte contre les infractions terroristes et les crimes graves. Or, le scandale Pegasus a montré les failles et les limites de ces projets qui, lorsqu'ils sont vendus à des régimes autoritaires, peuvent devenir des outils de surveillance de masse.

Bien que les États européens revendiquent un arsenal législatif permettant de protéger les droits fondamentaux de leurs citoyens, notamment le droit à la protection de la vie privée et des données à caractère personnel, le scandale Pegasus a également permis de révéler les limites de l'effectivité de ces outils juridiques. En effet, des membres d'une commission d'enquête du Parlement européen, après avoir effectué une visite en Israël, ont découvert que le logiciel incriminé continuait à être utilisé régulièrement « dans pas moins de 12 des 27 pays de l'Union européenne par 22 organismes de renseignements, de police et de justice »¹¹¹⁹. Les enquêtes réalisées par le consortium de journalistes du Monde ont révélé que le chef d'État espagnol, comme le Président français, ont été mis sur écoute. Le scandale Pegasus va au-delà du scandale des révélations d'Edward Snowden en 2013 sur les opérations de la NSA. Ici, les victimes du logiciel d'espionnage ont été ciblées individuellement par les gouvernements et les agences de renseignement. Mais les deux scandales ont une chose en commun : ils montrent que les espions qui utilisent les outils les plus sophistiqués pour surveiller et

¹¹¹⁷ Ibidem

¹¹¹⁸ Ibid.

¹¹¹⁹ M. HENRY, « Après le scandale des écoutes, NSO, le fabricant du logiciel espion Pegasus, fait un grand ménage », *Le Figaro*, 21 août 2022, en ligne à URL : <https://www.lefigaro.fr/secteur/high-tech/depart-du-pdg-de-nso-fabricant-du-controverse-logiciel-espion-pegasus-20220821> consulté le 3 juillet 2023.

contrôler les moindres détails de la vie de leurs cibles ne sont jamais tenus pour responsables¹¹²⁰.

Le 22 mai 2022, une commission d'enquête du Parlement européen, chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents, a publié un rapport sur l'impact du logiciel espion Pegasus sur les droits de l'Homme, lors d'une session d'été du Parlement¹¹²¹. Pour l'Union européenne, l'utilisation de technologies intrusives menace non seulement l'exercice effectif des droits fondamentaux tels que le droit à la vie privée et la liberté d'expression, mais érode également le concept d'autonomie individuelle. De plus, ces technologies peuvent compromettre l'intégrité physique des personnes. Les pratiques de surveillance ainsi mises en lumière risquent d'affaiblir les principes de l'État de droit et de porter atteinte à la crédibilité des institutions démocratiques.

Le Parlement européen souligne, dans ses recommandations sur ce sujet, que la sécurité nationale et la lutte contre les activités criminelles peuvent, dans des circonstances exceptionnelles, justifier l'utilisation de technologies de surveillance des communications. Les forces de l'ordre et les services de renseignement disposent en effet de motifs légitimes pour collecter les informations nécessaires à la protection publique. Cependant, l'exercice de ces pouvoirs doit être strictement encadré par les instruments internationaux, régionaux et nationaux relatifs aux droits de l'Homme, afin de prévenir tout abus et de garantir le respect des libertés fondamentales¹¹²².

En effet, la Convention 108+ précise dans son rapport interprétatif, à l'article 11, les principes et conditions à respecter dans ce contexte¹¹²³. La crainte pour les institutions démocratiques est que la surveillance secrète peut toujours laisser place à l'arbitraire et menacer la jouissance de fait d'un certain nombre de droits et de libertés fondamentales, notamment le droit au respect de la vie privée et familiale et des communications tels qu'énoncé par l'article 8 de la CEDH¹¹²⁴.

¹¹²⁰ D. LELOUP, M. UNTERSINGER, « 'Projet Pegasus' : révélations sur un système mondial d'espionnage de téléphones », *Le Monde*, 4 novembre 2022, en ligne à URL : https://www.lemonde.fr/projet-pegasus/article/2021/07/18/projet-pegasus-revelations-sur-un-systeme-mondial-d-espionnage-de-telephones_6088652_6088648.html?random=1430103654 consulté le 3 juillet 2023.

¹¹²¹ Parlement européen, « Rapport relatif à l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents », 22 mai 2023.

¹¹²² Parlement européen, « Recommandation du Parlement européen du 15 juin 2023 à l'intention du Conseil et de la Commission à la suite de l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents », 15 juin 2023.

¹¹²³ Convention 108 +, article 11.

¹¹²⁴ CEDH, article 8.

Ces outils de surveillance sont déjà utilisés dans de nombreux régimes autoritaires, comme en Arabie saoudite, pour traquer les opposants politiques et restreindre la liberté d'information et d'expression. Par conséquent, le développement et le déploiement des technologies de surveillance doivent être accompagnés de garanties juridiques appropriées et efficaces, afin d'assurer une protection adéquate des individus et de maintenir un équilibre juste entre les intérêts en jeu et les droits et libertés concernés. Cette approche doit également s'appliquer à la collecte et à l'utilisation des données personnelles des passagers aériens, dont le traitement est principalement destiné à la lutte contre le terrorisme et le crime organisé. Il est essentiel que l'utilisation de telles techniques intrusives ne compromette pas les droits fondamentaux des citoyens, même dans le cadre de la lutte contre des crimes graves.

Si la sécurité nationale peut justifier l'utilisation exceptionnelle des technologies de surveillance des communications et des transferts de données des passagers aériens, ces objectifs légitimes des agences en charge de la sécurité des citoyens européens doivent être encadrés par un cadre juridique clair et strict. Ce cadre est essentiel pour prévenir, d'une part, les atteintes à l'intégrité physique des individus et, d'autre part, les menaces à la crédibilité des institutions démocratiques ainsi qu'à l'État de droit, comme en a témoigné le scandale du logiciel Pegasus.

Sous-section 2 – Les transporteurs aériens face à la collecte massive des données personnelles des passagers aériens

L'augmentation continue des flux migratoires coïncide avec une réduction des ressources financières disponibles pour l'État. Face à ces contraintes, l'État ne peut plus se permettre d'agir de manière autonome, car ses moyens matériels et humains sont insuffisants. Il a donc été nécessaire de réviser sa méthode en intégrant des acteurs privés, qui, bien que soumis à divers degrés de contrôle public, apportent leur soutien au processus. Ainsi, l'État établit un cadre réglementaire et délègue à des entités privées le rôle de participer au contrôle des migrations.

Sur le fondement du droit européen, notamment les accords de Schengen, les États européens ont impliqué les transporteurs¹¹²⁵. L'annexe 9 de la Convention de Chicago du 7 décembre 1944 relative à l'aviation civile internationale insistait déjà sur les précautions à prendre « au point d'embarquement afin que les passagers soient en possession des documents prescrits par les États contractants aux fins de contrôle ». Par conséquent, les transporteurs aériens se sont retrouvés en première ligne pour réaliser des vérifications relatives aux conditions d'entrée

¹¹²⁵ K. LE BOURHIS, *Les transporteurs et le contrôle des flux migratoires*, L'Harmattan, 2001.

sur le territoire et l'État leur a progressivement imposé de transmettre des informations relatives aux passagers aériens qui alimentent ainsi des dossiers spécifiques.

§ 1 – Les transporteurs aériens comme professionnels du transport

Le transport aérien public est réglementé afin d'offrir des garanties en termes de sécurité, c'est pourquoi au sein de l'Union européenne, un transporteur doit respecter les exigences requises s'il veut exercer son activité. Le droit distingue le transport public du transport privé qui exclut tout caractère commercial¹¹²⁶. Le premier se définit comme le fait d'acheminer par aéronef des passagers, des marchandises ou du courrier, à titre onéreux, d'un point d'origine à un point de destination¹¹²⁷. Mises à part certaines exceptions, seules les entreprises qui disposent d'une licence d'exploitation et d'un certificat de transporteur aérien (CTA) délivrés par les autorités d'un État membre de l'Union européenne sont autorisés à transporter par voie aérienne, en contrepartie d'une rémunération, des passagers ou des marchandises¹¹²⁸.

En France, la Direction générale de l'aviation civile (DGAC)¹¹²⁹ est l'autorité chargée de délivrer ces autorisations qui permettent la création d'une compagnie aérienne. Une liste des compagnies aériennes françaises autorisées par la DGAC recense les transporteurs français qui détiennent un certificat de transporteur aérien et une licence d'exploitation¹¹³⁰.

Le transport privé s'entend comme celui organisé par une personne pour son propre compte, qui peut être publique ou privée. Ici, le vol ne peut être proposé à la vente et la prestation doit être proposée à titre gratuit ou bien selon le modèle des frais partagés. Le transport privé ne requiert pas la délivrance d'une autorisation préalable. Les exigences en matière de sécurité dans ce domaine font donc l'objet d'une surveillance moins étroite que dans le cas du transport public.

¹¹²⁶ L'article L1000-3 du Code des transports définit le transport public comme tout transport de personnes ou de marchandises, à l'exception de celui effectué pour le compte propre d'une personne, qu'elle soit publique ou privée, ou relevant d'une autre réglementation. De plus, les opérations de transport liées à un déménagement sont également considérées comme des transports de marchandises. L'article indique que la distinction entre transport public et transport privé repose sur le critère de l'organisation : le transport public est effectué pour le compte d'autrui, tandis que le transport privé est réalisé pour son propre compte.

¹¹²⁷ Gouvernement français, Définition, « Transport public ou privé », *Ministère de la Transition écologique et de la Cohésion des territoires – Ministère de la Transition énergétique*, en ligne à URL : <https://www.ecologie.gouv.fr/transport-public-ou-privé> consulté le 11 janvier 2023.

¹¹²⁸ Règlement (CE) n° 1008/2008, article 3.

¹¹²⁹ La direction générale de l'Aviation civile (DGAC) est en France l'administration, rattachée au ministère de la Transition écologique, qui regroupe l'ensemble des services de l'État chargés de réglementer et de superviser la sécurité aérienne, le transport aérien et les activités de l'aviation civile en général.

¹¹³⁰ Règlement (CE) n° 1008/2008, article 10. En France, la liste des compagnies aériennes autorisées, qui détiennent un certificat de transporteur aérien (CTA) et une licence d'exploitation, est publiée par la DGAC. Cette liste est disponible sur le site officiel de la DGAC.

Le transport public devient illicite (TPI) lorsqu'un transport aérien est réalisé contre rémunération sans détenir les autorisations requises comme le certificat de transporteur aérien ou la licence d'exploitation. Le transport public illicite est constitué lorsqu'une personne achète une prestation de transport et que celle-ci donne lieu à une facturation par une société non autorisée, autrement dit qui ne détient pas les autorisations associées, qu'il s'agisse d'une société ou d'un pilote seul. Dans ce cas, le niveau de sécurité n'est plus garanti et les transporteurs opérant un vol illégal sont passibles de poursuites pénales et administratives¹¹³¹.

§2 – Les transporteurs aériens face à l'émergence du droit européen

Avant l'émergence de la politique commune des transports aériens au sein de l'Union européenne, les transporteurs aériens ont vu leur cadre juridique consolidé par les règles internationales qui encadrent cette activité économique depuis ses origines. Le principal fondement de ce droit demeure l'Accord international sur le transit des services aériens, dit « Convention de Chicago », signé le 7 décembre 1944 et entrée en vigueur le 4 avril 1947¹¹³². Cette convention a donné naissance à une nouvelle institution à vocation internationale, sous l'égide des Nations unies, à savoir l'Organisation de l'aviation civile internationale (OACI). La Convention de Chicago réaffirme avant toute chose le principe selon lequel les États disposent d'une souveraineté exclusive sur la gestion de l'espace aérien au-dessus de leur territoire. Elle prend la suite de la Convention de Paris de 1919 relative à la navigation aérienne internationale et de la Convention de Varsovie de 1929 pour l'unification de certaines règles relatives au transport aérien international. La Convention de Chicago a vu son régime évoluer avec la Convention de Montréal, signée le 28 mai 1999 par 107 États parties et entrée en vigueur le 4 novembre 2003. Ce cadre permet aux États et aux opérateurs du secteur aérien de viser une uniformisation du droit international aérien¹¹³³.

Les membres de l'OACI, au nombre de 193 au 1^{er} septembre 2024¹¹³⁴, ont consenti à des libertés en tant que pays signataires dont la première est le droit de traverser le territoire d'un État signataire sans y faire escale et la seconde le droit d'atterrir sur ce territoire pour des raisons non commerciales. Trois autres libertés, à caractère commercial, étaient également prévues par un chapitre de la Convention mais ce chapitre n'est jamais entré en vigueur : le droit de débarquer des passagers, du courrier et des marchandises embarqués sur le territoire

¹¹³¹ Cour de Cassation, Chambre criminelle, 19 février 1997, n° 95-81352.

¹¹³² S. RODRIGUES, « Transports aériens », *Répertoire de droit européen*, mai 2022.

¹¹³³ O. CACHARD, *Le transport international aérien de passagers*, Académie de droit international de la Haye, 2015, p. 26.

¹¹³⁴ OACI, États membres, 1^{er} septembre 2024, en ligne à URL : https://www.icao.int/about-icao/Pages/FR/member-states_FR.aspx consulté le 1er septembre 2024.

de l'État où l'aéronef est immatriculé (3^e liberté), le droit d'embarquer des passagers, du courrier et des marchandises à destination du territoire de l'État où l'aéronef est immatriculé (4^e liberté) et le droit d'embarquer des passagers, du courrier et des marchandises à destination du territoire de tout autre État signataire combiné au droit de débarquer des passagers, du courrier et des marchandises en provenance du territoire de tout autre État signataire (5^e liberté)¹¹³⁵.

Trois autres libertés commerciales existent en pratique : le droit d'assurer des transports entre deux États différents de celui où l'aéronef est immatriculé à travers le territoire de ce dernier (6^e liberté), le droit d'opérer en dehors de l'État d'immatriculation ainsi que de débarquer ou embarquer des passagers, du courrier et des marchandises en provenance ou à destination d'un État tiers différent de celui de l'immatriculation (7^e liberté) et le droit de transporter des passagers, du courrier ou des marchandises d'un point à l'autre d'un État différent de celui où l'aéronef est immatriculé, qualifié aussi de « droit de cabotage » (8^e liberté). Ces différentes libertés commerciales sont régies à ce jour par des accords bilatéraux entre États. Ces derniers assurent la mise en œuvre de ces droits au cas par cas, selon un champ d'application plus ou moins large¹¹³⁶.

En droit européen, le TFUE prévoit une compétence partagée dans le domaine des transports entre l'Union européenne et les États membres, comme indiqué à l'article 4.2. Par ailleurs, l'article 90 précise que les objectifs des traités sont atteints par le biais d'une politique commune des transports, telle qu'encadrée par le titre VI de la troisième partie du traité. Ce titre prend en compte les spécificités du secteur des transports. L'article 91.1, dans le cadre de la procédure législative ordinaire, vise à établir des règles communes pour les transports internationaux, l'admission des transporteurs non-résidents, l'amélioration de la sécurité des transports, ainsi que d'autres mesures nécessaires¹¹³⁷.

L'article 91.2 TFUE ajoute que « lors de l'adoption de ces règles ou mesures, il doit être tenu compte des cas où l'application serait susceptible d'affecter gravement le niveau de vie et l'emploi dans certaines régions, ainsi que l'exploitation des équipements de transport ». Il existe également un régime particulier d'autorisation des aides accordées pour les besoins de la coordination des transports ou l'exécution de missions de service public, prévu à l'article 93 du TFUE. S'y ajoutent l'obligation de suppression de toute discrimination dans le transport de marchandises à l'intérieur de l'Union prévue à l'article 95 du TFUE, l'interdiction de principe

¹¹³⁵ S. RODRIGUES, « Transports aériens », *Répertoire de droit européen*, mai 2022.

¹¹³⁶ Ibidem

¹¹³⁷ Ibid.

de toute mesure étatique de soutien ou de protection au profit d'une entreprise de transport mentionnée à l'article 96 et la réduction progressive des taxes ou redevances perçues par un transporteur pour les frais de passage aux frontières indiquée à l'article 97 du Traité. Il convient de préciser que l'article 98 du TFUE prévoit, pour sa part, un régime dérogatoire au profit de la République Fédérale d'Allemagne pour compenser les désavantages économiques causés à l'économie de certaines de ses régions à cause de la division de son territoire. Ce régime dérogatoire est abrogé cinq ans après l'entrée en vigueur du Traité de Lisbonne, au 1^{er} décembre 2009. Ce dernier a introduit cette possibilité en prévoyant une décision du Conseil en ce sens, sur proposition de la Commission.

Dès 1957, le droit européen a établi une distinction entre les modes de transports pour leur appliquer des règles particulières. Alors que les dispositions du titre VI du TFUE s'appliquent de plein droit « aux transports par chemin de fer, par route et par voie navigable », comme le prévoit l'article 100.1, il n'en est pas de même pour la navigation maritime et aérienne. En effet, l'article 100.2 du TFUE énonce que « le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, peuvent établir les dispositions appropriées » pour ces deux modes de transport. La doctrine fait remarquer que dans la version originale du Traité de Rome, il était précisé que le législateur, jadis le seul Conseil, pouvait décider « si, dans quelle mesure et par quelle procédure des dispositions appropriées pourront être prises » dans ces secteurs¹¹³⁸. La principale conséquence de cette double précaution, à savoir la faculté du législateur et le caractère approprié de la réglementation, a été une lente élaboration de la politique commune européenne des transports aériens. Les États membres préféraient plus aisément le statu quo et le confort de la souveraineté nationale au détriment des perspectives supposées non contrôlées d'un marché intérieur de la navigation aérienne.

Aujourd'hui, le droit européen des transports aériens se fonde sur les règles du Traité, notamment les règles de la concurrence et de libre circulation, sans s'y limiter. Il s'adresse à plusieurs acteurs dont les transporteurs, les passagers, les riverains des aéroports et les autorités nationales. Les transporteurs aériens ont été les premiers et demeurent certainement les principaux acteurs économiques de la réalisation du marché unique aérien compte tenu du fait qu'ils ont eu à la fois à s'adapter aux normes techniques et sociales régissant leur activité et à intégrer dans leurs comportements les exigences du marché intérieur¹¹³⁹. Les normes

¹¹³⁸ Ibid.

¹¹³⁹ R. GÖNENÇ, G. NICOLETTI, « Le transport aérien de passagers : réglementation, structure du marché et performance », *Revue économique de l'OCDE*, 2001/1, p.203-254.

techniques, notamment en matière de sécurité, ont progressivement été harmonisées à l'échelon de l'Union européenne¹¹⁴⁰. La sécurité est une exigence essentielle pour le transporteur aérien dans l'exercice de ses activités. Le règlement n° 216/2008 est clair à cet égard en énonçant explicitement que son objectif principal est « d'établir et de maintenir un niveau uniforme élevé de sécurité de l'aviation civile en Europe » (art. 2-1)¹¹⁴¹.

Les attentats du 11 septembre 2001 ont généré un intérêt accru pour les dossiers passagers dont les compagnies aériennes disposent pour chaque voyage réservé par un passager¹¹⁴². Ces fichiers sont stockés sur les bases de données de réservation et de contrôle des départs des compagnies aériennes et permettent à tous les intervenants du secteur aérien (notamment l'agence de voyage, les agents d'assistance en escale dans les aéroports en passant par les systèmes informatisés de réservation et les transporteurs aériens) de reconnaître chaque passager et d'avoir accès à toutes les informations pertinentes concernant son voyage comme les vols aller et retour, les vols de correspondance et services particuliers demandés à bord, entre autres¹¹⁴³. Différents outils juridiques, notamment la directive européenne sur le PNR mais également les accords bilatéraux entre l'Union européenne et plusieurs États, comme les États-Unis et le Canada, sont venus ajouter des obligations reposant sur les transporteurs aériens, au nom de considérations mondiales de sécurité de l'aviation civile.

En matière de sécurité aérienne, les transporteurs sont donc confrontés au défi de l'articulation d'ordres juridiques : ordre juridique supranational, ordre juridique de l'Union européenne et ordres juridiques nationaux.

§3 – Les transporteurs aériens comme utilisateurs des données personnelles

Deux obligations s'imposent aux transporteurs selon le cadre juridique actuel : le contrôle des documents de voyage et la transmission de données relatives aux voyageurs aux autorités étatiques¹¹⁴⁴. En France, la loi n° 92-190 du 25 février 1992, puis le Code de l'entrée et du séjour des étrangers et du droit d'asile (CESEDA), obligent les autorités compétentes à

¹¹⁴⁰ S. RODRIGUES, « Transports aériens », *Répertoire de droit européen*, mai 2022.

¹¹⁴¹ Règlement n° 216/2008 du Parlement européen et du Conseil, 20 février 2008, JOUE, n° L 79, 19 mars, concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence européenne de la sécurité aérienne, et abrogeant la Directive n° 91/670 du Conseil, le Règlement n° 1592/2002 et la Directive n° 2004/36, tel que modifié, en dernier lieu, par le Règlement n° 6/2013 de la Commission, 8 janvier 2013, JOUE, no L 4, 9 janvier.

¹¹⁴² H. MOUTOUH, J. POIROT, « PNR (Passenger Name Record) », in *Dictionnaire du renseignement*, Perrin, 2018.

¹¹⁴³ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

¹¹⁴⁴ X. LATOUR, « La participation des personnes privées au contrôle des migrations en France », *Actualité Juridique Droit Administratif*, Dalloz, 2019, p. 264.

vérifier les documents de voyage des personnes transportées, ressortissants d'États tiers à l'UE, dès qu'ils s'inscrivent dans une relation commerciale, comme l'a rappelé la jurisprudence française¹¹⁴⁵. Le CESEDA régit les transporteurs aériens et maritimes à travers l'article L. 625-1 et les autocaristes internationaux à l'article L. 625-6. En cas de violation de leurs obligations, les articles L. 213-4 à L. 213-8 obligent les transporteurs à réacheminer, à leurs frais, les passagers en situation irrégulière. Ces derniers doivent également s'acquitter d'une amende qui est susceptible d'un recours de pleine juridiction, sur le fondement de la directive 2001/51/CE du Conseil du 28 juin 2001 visant à compléter les dispositions de l'article 26 de la Convention d'application de l'accord de Schengen du 14 juin 1985.

Ce cadre juridique s'inscrit dans le contexte d'ouverture des frontières intérieures européennes avec les accords de Schengen du 19 juin 1991 qui a requis une meilleure coordination de ces États face aux flux migratoires non canalisés. La doctrine rappelle toutefois que cette préoccupation date en France d'avant Schengen puisque dès 1966, à travers la loi n° 66-420 du 18 juin 1966¹¹⁴⁶ sur les contrats d'affrètement et de transport maritime, le droit français faisait peser une responsabilité sur les compagnies maritimes¹¹⁴⁷. Dans le secteur du rail, la Convention de Berne relative aux transports internationaux ferroviaires du 9 mai 1980 impose aux voyageurs de se soumettre aux prescriptions administratives ; toutefois, elle ne prévoit aucun mécanisme de responsabilité du transporteur. Par ailleurs, dans un souci de protection des voyageurs, la jurisprudence française a considéré les zones de transit comme appartenant au territoire national¹¹⁴⁸.

En principe, les transporteurs n'exercent pas de pouvoir de police puisque les vérifications qu'ils effectuent « n'ont pas pour projet et ne sauraient avoir pour effet de conférer au transporteur un pouvoir de police au lieu et place de la puissance publique, elles obligent de vérifier que l'étranger est muni des documents de voyage et des visas éventuellement requis, et que ceux-ci ne comportent pas des éléments d'irrégularité manifeste, décelables par un examen normalement attentif des agents de la compagnie »¹¹⁴⁹. Néanmoins, la doctrine considère que les transporteurs peuvent être envisagés comme des « postes avancés au

¹¹⁴⁵ CAA Paris, 12 avr. 2010, n° 08PA05060, *ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales c/ Société V. Ships*, AJDA 2010, 1446.

¹¹⁴⁶ Loi n° 66-420 du 18 juin 1966 sur les contrats d'affrètement et de transport maritimes, article 34.

¹¹⁴⁷ X. LATOUR, Op. cit.

¹¹⁴⁸ CE, 7 déc. 2005, n° 271569, *ministère de l'Intérieur et de l'aménagement du territoire c/ Société Air France, Lebon*, AJDA 2006, 754, concl. I. de Silva.

¹¹⁴⁹ CAA Paris, 10 févr. 1998, n° 96PA02799, *Compagnie nationale Air France, Lebon*, AJDA 1998, 280 ; et 227.

service » de la France dans les territoires de départ d'où s'envolent les passagers¹¹⁵⁰. Leur fonction est alors d'agir en partenariat avec les services de police. Ils sont assistés par l'État avec qui ils effectuent des échanges d'informations pouvant porter, à titre d'illustration, sur des cas de falsification de documents¹¹⁵¹.

L'échange de données sur les passagers aériens aux forces publiques de sécurité est l'une des autres formes de partenariat entre les transporteurs aériens et l'État. Aussi bien à l'international qu'en France, les transporteurs ont l'obligation de collecter ces données pour les transférer aux forces de sécurité¹¹⁵². Les données des passagers aériens – PNR – permettent aux autorités étatiques de lutter contre la pression terroriste et le crime organisé en anticipant, avec l'assistance des transporteurs, l'arrivée de personnes indésirables sur leur territoire. L'activité des transporteurs est ainsi inscrite dans un cadre juridique, dont le droit européen est devenu l'une des sources avec la directive PNR, qui contraint les compagnies opérant dans les États de départ à transférer les informations aux autorités compétentes des États de destination¹¹⁵³.

Les services répressifs de l'État, en recevant ces informations des transporteurs, peuvent utiliser les données PNR pour les comparer à celles des systèmes d'alerte afin d'identifier des terroristes et des criminels connus, un passager ayant des liens avec l'individu connu pour des infractions de terrorisme ou de crime organisé dans le cas où sont utilisés la même adresse, un même numéro de carte de crédit ou les mêmes coordonnées, démarche utile dans le cas d'une association de criminels. Les données PNR sont croisées avec deux éléments principaux : d'une part, un ensemble de caractéristiques et de comportements pour évaluer les risques, et d'autre part, des renseignements sur les risques pertinents à un moment précis afin de repérer les passagers à haut risque¹¹⁵⁴.

Les données PNR peuvent aussi être comparées à d'autres informations pour identifier l'agence de voyage installée dans un pays à haut risque et qui a des liens avec une organisation terroriste ou une association de criminels. Les données des passagers aériens permettent d'aider à identifier les passagers qui ont acheté leur billet auprès de l'agence soupçonnée d'une activité criminelle. Ces données permettent également de fournir des

¹¹⁵⁰ X. LATOUR, « La participation des personnes privées au contrôle des migrations en France », *Actualité Juridique Droit Administratif*, Dalloz, 2019, p. 264.

¹¹⁵¹ Ibidem

¹¹⁵² Ibid.

¹¹⁵³ Commission des communautés européennes, *Résumé de l'analyse d'impact*, Document de travail des services de la commission accompagnant la Décision-cadre du Conseil relative à l'utilisation de données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives, Com(2007), 654 final, 2007.

¹¹⁵⁴ Ibidem

renseignements sur les schémas de déplacement des passagers à risques et les associations dans le cas où une infraction terroriste est perpétrée¹¹⁵⁵.

Aujourd'hui, le droit européen, transposé ou appliqué directement par les États membres, vise à harmoniser leurs dispositions en faisant obligation aux transporteurs aériens, qui assurent des vols entre un pays tiers et le territoire d'au moins un État membre, de transmettre aux autorités compétentes les données PNR aux fins de prévention et de détection des infractions terroristes et des infractions graves, ainsi que des enquêtes et des poursuites y afférentes¹¹⁵⁶. Tous les traitements de données PNR effectués dans le cadre du droit européen se doivent d'appliquer des normes élevées conformément à la Charte des droits fondamentaux de l'Union européenne, la Convention 108 et la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales. Ces normes forment un cadre solide qui protège les droits fondamentaux des Européens dans un contexte de développement rapide des nouvelles technologies.

Les traitements de données personnelles des passagers aériens réalisés par les transporteurs ne se fondent pas sur l'origine raciale ou ethnique, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à un syndicat, la santé, la vie sexuelle ou l'orientation sexuelle d'une personne¹¹⁵⁷. En effet, les données PNR sont réputées ne comporter que des informations relatives aux réservations et aux itinéraires de voyage des passagers, permettant aux autorités compétentes d'identifier les passagers aériens qui sont susceptibles de présenter une menace pour la sécurité intérieure du pays.

Ces principes rappelés, les transporteurs sont appelés à prendre les mesures nécessaires pour protéger les droits et libertés des passagers aériens faisant l'objet de la collecte. Cependant, les transporteurs aériens ne sont pas à l'abri d'attaques susceptibles d'entraîner une fuite d'informations personnelles sur les voyageurs. C'est pourquoi, la Convention de Chicago¹¹⁵⁸ rappelle à cet effet l'impératif de protection de « la confidentialité, l'intégralité et la disponibilité des systèmes et données informatiques et de communications critiques utilisées aux fins de l'aviation civile ». Cette prévention est difficile à assurer au regard de l'interconnexion de plusieurs bases de données induite par la mise en place de dispositifs censés offrir un parcours de voyage plus fluide et simplifié aux voyageurs, tout en

¹¹⁵⁵ Ibid.

¹¹⁵⁶ Directive 2016/681/UE 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.

¹¹⁵⁷ Ibidem.

¹¹⁵⁸ Convention relative à l'aviation civile internationale, Chicago, le 7 décembre 1944.

garantissant leur sécurité et celle de leurs biens. Les transporteurs aériens ne doivent pas être insensibles aux critiques émises par le Contrôleur européen de la protection des données qui n'avait pas été « convaincu par les éléments démontrant la nécessité et la proportionnalité du traitement massif et quotidien des données concernant les passagers qui ne sont pas considérés par les services de police comme suspects »¹¹⁵⁹.

Section 2 – Un profilage des passagers aériens en conflit avec le droit à la vie privée et la protection des données personnelles

L'article 4 du RGPD définit le profilage comme toute forme de traitement automatisé de données à caractère personnel dont l'objet est d'utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour prédire et analyser des éléments qui concernent le comportement, la localisation, la situation économique, la santé, les intérêts, la fiabilité ou les préférences personnelles ou les déplacements de cette personne¹¹⁶⁰. Cette opération ne signifie pas une prise de décision automatisée en ce qu'une intervention humaine est possible. *A contrario*, la prise de décision automatisée n'est pas nécessairement synonyme de profilage si elle n'a pas pour objet d'évaluer des aspects personnels d'une personne physique. Ainsi, ne constitue pas un profilage une classification à des fins statistiques de clients en fonction de leur âge¹¹⁶¹.

La recommandation 2010/13 du Conseil de l'Europe précise que le profilage est défini à la lumière des trois critères suivants : la collecte de données, un traitement automatisé pour établir des corrélations et l'usage de ces corrélations pour identifier les caractéristiques de comportements actuels ou futurs¹¹⁶². La doctrine retient deux approches du profilage à l'aune du RGPD. La première, *lato sensu*, considère que le profilage existe lorsque « le traitement automatisé n'a d'autre but que d'analyser les données ou évaluer les comportements individuels en l'absence de toute prédiction établie sur la base de la segmentation ou des corrélations effectuées »¹¹⁶³. La seconde, *stricto sensu*, considère que le profilage « suppose nécessairement à la fois un traitement automatisé et une prise de décision automatisée,

¹¹⁵⁹ CEPD, « Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data », 30 septembre 2013, considérant 3.

¹¹⁶⁰ Article 4, Règlement général sur la protection des données.

¹¹⁶¹ Fiche d'orientation, *Profilage*, Dalloz, septembre 2022.

¹¹⁶² Council of Europe, *The protection of individuals with regard to automatic processing of personal data in the context of profiling*, Recommendation CM/Rec (2010) 13 and explanatory memorandum, Council of Europe, 23 November 2010.

¹¹⁶³ N. MARTIAL-BRAZ, « Le profilage, fiche pratique », *Communication Commerce électronique*, n° 4, Dossier 15, LexisNexis, avril 2018.

autrement dit sans aucune intervention humaine »¹¹⁶⁴. La doctrine semble favoriser l'acceptation stricte du profilage bien que les termes de la définition proposée par le RGPD laissent entendre une approche aux contours larges¹¹⁶⁵. En plus d'être régie par les dispositions du RGPD, cette opération est encadrée par les règles qui régissent le traitement des données personnelles des passagers aériens lorsqu'elle porte sur celles-ci.

À titre de comparaison, la directive (UE) 2016/680 du Parlement européen et du Conseil¹¹⁶⁶ interdit l'adoption d'une décision qui soit fondée exclusivement sur un traitement automatisé, y compris le profilage, et qui produit des effets juridiques « défavorables » ou qui affecte la personne concernée de « manière significative », sauf si elle est assortie de garanties appropriées et d'être autorisée par le droit européen ou par le droit d'un État membre¹¹⁶⁷. À l'instar des acteurs privés, les autorités étatiques peuvent procéder à du « datamining »¹¹⁶⁸. Cette technique permet à l'aide d'algorithmes de croiser certaines données et d'établir des profils particuliers ou d'anticiper des comportements¹¹⁶⁹. La personne concernée dispose de droits en cas de décision automatisée. Elle peut obtenir des informations spécifiques, demander à une personne humaine la possibilité d'exprimer son point de vue et d'obtenir de l'autorité compétente une explication. À la différence du RGPD, la décision automatisée ne doit pas uniquement prévoir des effets juridiques mais ceux-ci doivent être « défavorables » selon l'article 22, § 1 du règlement.

Pour permettre la garantie de l'effectivité des droits de la personne concernée, l'autorité compétente doit être en mesure de modifier la décision et d'examiner les données pertinentes, y compris celles que l'intéressé a fournies. C'est ainsi que dans la directive PNR, il est permis l'exploration systématique de données dans le but de « situer » des passagers selon le degré de risques et d'ainsi identifier des individus recherchés pour des crimes « éventuels ou probables » sans lien avec une enquête spécifique¹¹⁷⁰.

¹¹⁶⁴ Ibidem

¹¹⁶⁵ Ibid.

¹¹⁶⁶ 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.

¹¹⁶⁷ C. FORGET, « La protection des données dans le secteur de la police et de la justice », *Larcier*, Le règlement général sur la protection des données, Dalloz, 2018.

¹¹⁶⁸ Le « datamining » est l'analyse de données depuis différentes perspectives et le fait de transformer ces données en informations utiles, en établissant des relations entre les données ou en repérant des tendances.

¹¹⁶⁹ C. FORGET, op. cit.

¹¹⁷⁰ Ibidem

Toutefois, l'article 6, §5 de la directive PNR impose aux États membres de s'assurer que toute concordance positive relevée à la suite d'un traitement automatisé des données des passagers aériens fasse l'objet d'une vérification individuelle par des moyens non-automatisés, dans le but de vérifier si des mesures effectives doivent être prises conformément au droit national¹¹⁷¹. Ces précautions n'ont pas évité des critiques de la directive, notamment par le Conseil et le CEPD, respectivement dans le rapport du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé du Conseil de l'Europe¹¹⁷² et l'avis n° 5/2015 du CEPD¹¹⁷³.

Sous-section 1 – Le profilage face aux règles régissant le traitement des données à caractère personnel

Le profilage se présente comme une opération catégorisant les individus en fonction de leurs caractéristiques propres. Lorsque les agents chargés de la gestion des frontières et les autorités policières collectent et traitent des données personnelles, elles doivent s'assurer que cette collecte et ce traitement disposent d'une base légale, d'un objectif valide et légitime et qu'ils soient nécessaires et proportionnés¹¹⁷⁴.

Des caractéristiques protégées telles que la race, l'origine ethnique, le sexe ou la religion peuvent figurer parmi les critères que les autorités policières et les agents des frontières prennent en compte dans l'exercice de leurs pouvoirs mais elles ne peuvent constituer la base unique ou principale de distinction d'individus.

Le profilage basé principalement sur une ou plusieurs caractéristiques protégées constitue une discrimination directe et enfreint donc les droits et libertés des citoyens. Pour être licites, les contrôles et les renvois aux inspections frontalières de deuxième ligne doivent être fondés sur des bases raisonnables.

¹¹⁷¹ Article 6, §5 de la directive 2016/681/UE 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.

¹¹⁷² Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé, "Passenger Name Records, Data Mining & Data Protection: The Need for Strong Safeguards", Strasbourg, 15 juin 2015, T-PD(2015)11, préparé par Douwe Korff, avec avis de Marie Georges.

¹¹⁷³ CEPD, Avis n° 5/2015 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers 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, 24 septembre 2015.

¹¹⁷⁴ Agence des droits fondamentaux de l'Union européenne, « Guide pour la prévention du profilage illicite aujourd'hui et demain », 2019, en ligne à URL : https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_fr.pdf consulté le 28 juin 2023.

§ 1 – L’encadrement juridique du profilage par le Règlement général sur la protection des données

Historiquement, le droit français encadrait déjà les pratiques de profilage qui à l’époque concernaient l’Administration, avant d’être étendues au secteur privé¹¹⁷⁵. Sous l’empire du droit antérieur, la loi n’interdisait pas le traitement automatisé de données avec prise de décision automatique, notamment fondée sur le profil, dès lors que cette opération avait été adoptée dans le cadre de la conclusion ou de l’exécution d’un contrat ou lorsque la personne concernée avait été mise en capacité de pouvoir présenter ses observations¹¹⁷⁶. Dans ce contexte, la CNIL n’était pas sévère s’agissant de l’application de l’article 10 de la loi Informatique et Libertés. En effet, celle-ci se contentait de la « seule exigence d’un réexamen humain des refus prononcés sur le fondement d’un traitement en se préoccupant finalement peu des résultats concrets de celui-ci »¹¹⁷⁷. L’adoption du RGPD a fait évoluer le cadre juridique européen sur le profilage en apportant plus de précisions sur la manière avec laquelle les autorités compétentes devraient agir vis-à-vis du profilage.

L’article 22, paragraphe 1 du RGPD impose une interdiction spécifique concernant le profilage lorsqu’il est utilisé pour prendre des décisions exclusivement basées sur un traitement automatisé, notamment le profilage, qui aurait des effets juridiques ou des conséquences significatives pour l’individu. Cette interdiction ne s’applique pas à toutes les formes de profilage, mais uniquement lorsque le traitement automatisé mène à une décision qui a un impact juridique ou significatif sur la personne concernée. Les conditions pour que cette interdiction s’applique doivent être cumulativement remplies¹¹⁷⁸.

Les commentaires du G29 précisent le caractère pleinement automatique de l’interdiction du profilage, qui suppose qu’aucun rôle actif n’est nécessaire, de la part de la personne concernée, pour pouvoir en bénéficier. En effet, le RGPD vise bien à octroyer à la personne concernée le droit de ne pas faire l’objet d’une décision automatisée fondée sur un traitement

¹¹⁷⁵ Loi Informatique et Libertés de 1978 a établi les principes fondamentaux relatifs à la collecte, au traitement et à la protection des données personnelles en France. Bien qu’elle ne mentionne pas explicitement le profilage, elle posait les bases pour la protection des droits des individus en matière de traitement automatisé des données.

¹¹⁷⁶ N. MARTIAL-BRAZ, « Le profilage, fiche pratique », *Communication Commerce électronique*, n° 4, Dossier 15, LexisNexis, avril 2018.

¹¹⁷⁷ A. DEBET, « Profilage – APB enfin remis en cause ! », *Communication Commerce électronique*, Dalloz, 2017.

¹¹⁷⁸ Article 6, §5 de la directive 2016/681/UE 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.

automatisé, dont notamment le profilage, et qui produit des effets juridiques ou similaires l'affectant de manière notable¹¹⁷⁹.

Le principe d'interdiction prévu par l'article 22, §1 est tout d'abord fondé sur le fait que la prise de décision repose exclusivement sur un traitement automatisé. Autrement dit, absolument aucune intervention humaine sur la chaîne de traitement ne doit être présente. Ce critère permet de distinguer les profilages interdits de ceux qui, bien qu'autorisés, devront faire l'objet de mesures spéciales notamment en termes de droit d'opposition offert à la personne concernée. D'après les lignes directrices du G29, l'intervention humaine doit apporter une incidence concrète sur la prise de décision et être le fait d'une personne qui a autorité ou compétence pour changer la décision automatisée. L'étude d'impact, obligatoire dans ce cas, doit relever le degré d'implication humaine dans la décision prise¹¹⁸⁰.

Le principe d'interdiction se fonde ensuite sur la nécessité que cette prise de décision entièrement automatisée crée un effet juridique pour la personne concernée ou des effets similaires entraînant des conséquences significatives sur elles. Martial-Braz définit les effets juridiques comme l'ensemble « des conséquences sur les droits ou le statut des personnes à l'instar des décisions permettant de bénéficier ou non d'un statut social ou d'un contrat »¹¹⁸¹. Les exemples cités par le G29 sur les conséquences juridiques se caractérisent par l'existence d'un pouvoir contraignant au bénéfice ou au préjudice de la personne concernée. Les contours des effets similaires sont plus difficiles à cerner¹¹⁸².

L'article 22 §2 du RGPD prévoit plusieurs exceptions à l'interdiction du profilage automatisé¹¹⁸³. Cette interdiction ne s'applique pas lorsque la décision est nécessaire pour conclure ou exécuter un contrat avec la personne concernée, ou lorsqu'elle est autorisée par le droit de l'Union ou d'un État membre, à condition que des mesures appropriées soient en place pour protéger les droits et intérêts de l'individu. De plus, elle peut être levée si la personne concernée donne son consentement explicite. Ces exceptions permettent de justifier l'utilisation de décisions entièrement automatisées, même lorsqu'elles ont des effets significatifs sur l'individu.

¹¹⁷⁹ Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, Groupe de Travail « article 29 » sur la protection des données, 6 février 2018.

¹¹⁸⁰ N. MARTIAL-BRAZ, « Le profilage, fiche pratique », *Communication Commerce électronique*, n° 4, Dossier 15, LexisNexis, avril 2018.

¹¹⁸¹ Ibidem

¹¹⁸² Ibid.

¹¹⁸³ RGPD, article 22 §2.

La première exception est que la nécessité du contrat peut devenir une base de traitement licite. Le G29 l'interprète de manière stricte en considérant qu'il n'y aura nécessité de contrat que lorsque le profilage est le moyen le plus approprié pour parvenir à réaliser l'objectif déterminé¹¹⁸⁴. La seconde exception vise la législation de l'Union ou d'un État membre qui permet de déroger à l'interdiction, sous réserve de respecter les conditions restrictives posées par l'article 23, en disposant d'une des facultés d'adaptation et d'aménagement laissées aux États membres. La dernière exception est l'exigence d'un consentement explicite et éclairé qui est mis en perspective par la doctrine avec une obligation d'information pesant sur le responsable de traitement¹¹⁸⁵.

Ces exceptions ne s'appliquent pas dans le cas d'un traitement de données sensibles, telles que les données visées à l'article 9 du RGPD, sauf en cas de consentement explicite de la personne concernée ou pour des motifs d'intérêt public conséquents, si le responsable de traitement met en place des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée¹¹⁸⁶.

Le profilage illicite peut saper la confiance dans les gardes-frontières et la police. Aussi, cette opération peut conduire à un raidissement de la relation entre ces autorités publiques et les membres de communautés minoritaires qui peuvent se sentir marginalisées. Ce sentiment d'injustice peut saper la confiance que certains individus et groupes ont envers la police et les autres autorités, les conduisant éventuellement à moins signaler les crimes à la police et à moins coopérer avec les autorités. À leur tour, les autorités peuvent entretenir une certaine méfiance à l'égard de certains groupes, ce qui peut conduire à davantage de profilage illégal.

Le profilage illégal peut compromettre l'efficacité du profilage, car la fréquence à laquelle les individus sont contrôlés par la police ou à la frontière ne correspond pas nécessairement à la fréquence de la criminalité au sein des différents groupes.

Lorsque les minorités sont ciblées de manière disproportionnée par les forces de l'ordre ou les agents des frontières, il existe un risque de prophétie auto-réalisatrice, entraînant une augmentation des arrestations ou des inspections aux frontières. Le profilage illégal entraîne des conséquences juridiques et financières et les agents peuvent être tenus pour responsables. La police et les responsables de la gestion des frontières sont chargés d'assurer le profilage

¹¹⁸⁴ Groupe « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 6 février 2018.

¹¹⁸⁵ N. MARTIAL-BRAZ, « Le profilage, fiche pratique », *Communication Commerce électronique*, n° 4, Dossier 15, LexisNexis, avril 2018.

¹¹⁸⁶ Article 22, §4, Règlement général sur la protection des données.

conformément à la législation en vigueur. La collecte de données fiables, actuelles et exactes est essentielle pour assurer une responsabilité effective. Des mécanismes de plainte efficaces peuvent à la fois dissuader les abus de pouvoir et aider à restaurer la confiance du public envers les opérations de la police et des autorités de gestion des frontières. Les échanges avec les citoyens ont fourni des leçons importantes et amélioré les actions analytiques de ce type d'opération.

Le profilage algorithmique est tenu de respecter des règles spécifiques en matière de protection de données à caractère personnel¹¹⁸⁷. Lors de la conceptualisation et de la mise en œuvre de ce type de profilage¹¹⁸⁸, des biais peuvent être trouvés à chaque étape de ladite opération. Afin d'éviter cette situation et les éventuelles violations des droits fondamentaux qui en résultent, les informaticiens et les analystes en data doivent avoir une compréhension claire des droits fondamentaux¹¹⁸⁹. L'utilisation de données fiables est ainsi essentielle. Sinon, l'introduction de données dans un algorithme qui reflète les biais existants ou provient de sources non fiables produira des résultats biaisés et non fiables. C'est pourquoi l'opération de profilage doit être nécessaire, légitime et proportionnée.

Aussi, le traitement des données à caractère personnel doit avoir une finalité spécifique¹¹⁹⁰. De plus, les individus doivent, en recevant des informations sur les données à caractère personnel qui sont collectées et stockées, d'être informés sur le traitement, ses finalités et leurs droits. Ainsi, les données à caractère personnel des passagers aériens doivent être collectées, traitées et stockées dans un espace sûr¹¹⁹¹. Les autorités compétentes doivent conserver une trace des activités de traitement, y compris de ce qui est fait aux données personnelles, et des registres qui les concernent, y compris les informations sur les individus ayant accès aux données. Le traitement illicite de données doit être prohibé et détecté

¹¹⁸⁷ Agence des droits fondamentaux de l'Union européenne, *Guide pour la prévention du profilage illicite aujourd'hui et demain*, 2019. Cette entité européenne conseille les décideurs européens et nationaux sur les droits fondamentaux dans des domaines tels que le racisme et l'accès à la justice, voir <http://www.fra.europa.eu/fr>.

¹¹⁸⁸ W. MAXWELL, « Le contrôle humain des systèmes algorithmiques - un regard critique sur l'exigence d'un 'humain dans la boucle' », Droit, Université Paris 1 Panthéon- Sorbonne, 2022.

¹¹⁸⁹ L. CLUZEL-METAYER, « Calculer : l'influence des algorithmes sur l'édiction des décisions administratives », in Benoît Plessix (dir.), *Les méthodes en droit administratif*, Dalloz, 2018.

¹¹⁹⁰ RGPD, Chapitre 2. Voir aussi M. DE FALLOIS, « Les traitements de données de santé à des fins de recherche liés à la COVID-19 : quelle régulation par la CNIL ? », *Journal du droit de la santé et de l'assurance – Maladie*, 2021, pp. 26-32.

¹¹⁹¹ Agence des droits fondamentaux de l'Union européenne, « Guide pour la prévention du profilage illicite aujourd'hui et demain », 2019, en ligne à URL : https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_fr.pdf consulté le 28 juin 2023.

préalablement par des analyses d'impact ainsi que par l'utilisation d'outils de protection de la vie privée intégrés dans l'algorithme dès sa conception¹¹⁹².

§ 2 – Les droits des personnes concernées selon le Règlement général sur la protection des données

La personne concernée dispose de droits qu'elle peut faire prévaloir envers le responsable de traitement qui crée le profil. Elle peut également exercer ses droits à l'encontre de l'autorité qui prend une décision automatique sur la base de ce profil, qu'une décision humaine soit réalisée ou non, lorsqu'il s'agit de deux personnes distinctes. Le RGPD consacre un véritable droit aux personnes concernées permettant de limiter le profilage. Cependant, il est important de noter que l'application de ce droit varie en fonction des types de profilage. Martial-Braz souligne que cette mesure est interprétée différemment selon la nature du profilage en question¹¹⁹³. Elle est souvent décrite comme ayant des effets juridiques significatifs lorsqu'elle repose uniquement sur un traitement automatisé destiné à évaluer ou prévoir divers aspects personnels de l'individu, tels que son rendement professionnel, sa situation économique, sa localisation, son état de santé, ses préférences, sa fiabilité ou son comportement. En effet, à l'ère du numérique, des plateformes, des réseaux sociaux et des blogs, les individus ne cessent de dévoiler, sans toujours en avoir pleinement conscience, des séquences non-négligeables de leur vie privée¹¹⁹⁴.

Ces informations sont récoltées par les acteurs du numérique, notamment les plateformes, qui vont pouvoir personnaliser les services réalisés pour leurs clients ou leur fournir un soutien à la prise de décision, grâce aux algorithmes prédictifs ou à caractère décisionnel. Techniquement, ces programmes informatiques « qui exécutent instantanément une succession de calculs mathématiques permettent d'analyser et d'interpréter une quantité invraisemblable de données » qui viennent de diverses sources¹¹⁹⁵. Valorisées, ces données ont créé une volumineuse économie de la donnée d'où sont nées les grandes entreprises du numérique comme Google. Dans ce contexte, le profilage, lorsqu'il est utilisé pour évaluer et analyser les données d'une personne afin d'orienter les publicités selon les centres d'intérêt ou de prévenir certains comportements illicites, peut être source d'abus ou d'erreur¹¹⁹⁶. Ce travers est illustré par un « faux » tweet qui a fait perdre au Dow Jones près de 150 points, en

¹¹⁹² Ibidem.

¹¹⁹³ N. MARTIAL-BRAZ, « Le profilage, fiche pratique », *Communication Commerce électronique*, n° 4, Dossier 15, LexisNexis, avril 2018.

¹¹⁹⁴ C. FERAL-SCHUHL, « Des droits de la personne renforcés », *Les données personnelles*, Praxis Cyberdroit, Dalloz, 2020-2021.

¹¹⁹⁵ Ibidem

¹¹⁹⁶ Ibid.

quelques secondes, après que le compte de l'agence Associated Press a annoncé des explosions à la Maison Blanche. Or, ce tweet n'a été possible qu'après le piratage du compte d'agences de presse au niveau mondiale par des hackers. Ces derniers ont réussi à écrire sur ce compte que la Maison Blanche avait fait l'objet de deux explosions dans lesquelles le président américain Barack Obama avait été blessé. Cette manipulation d'algorithmes avec des mots clés comme « Maison Blanche », « Obama » et « explosion » a provoqué une perte de capitalisation boursière de l'ordre de 150 milliards de dollars¹¹⁹⁷. La réforme européenne du droit de la protection des données à caractère personnel devait régler de telles dérives en mettant la lumière sur l'existence des décisions automatisées et fournir à cet effet toutes informations utiles relatives à la logique sous-jacente à ce procédé. Les personnes concernées doivent également être informées sur les conséquences de ce traitement et leur droit de s'y opposer¹¹⁹⁸.

Avec le RGPD, le responsable de traitement, autrement dit la personne morale ou physique qui détermine les finalités et les moyens d'un traitement¹¹⁹⁹, est soumis à une obligation de transparence accrue¹²⁰⁰. Cette obligation du responsable de traitement donne droit à la personne concernée d'être informée de l'existence d'un profilage, *a minima* des « informations utiles concernant la logique sous-jacente, ainsi que de l'importance des conséquences prévues de ce traitement pour la personne concernée »¹²⁰¹, comme cela est prévu aux articles 13 et 14 du RGPD. L'article 15 prévoit le droit d'obtenir du responsable du traitement la confirmation ou non que la personne concernée fait l'objet d'un profilage.

D'autres droits sont consacrés comme celui de l'effacement, à l'article 17, §1, c), opérant un renvoi explicite aux conditions de l'article 21. Ce droit à l'effacement, contrairement aux réflexions portées sur le droit à l'oubli, permet de réaliser l'effacement des données dont le

¹¹⁹⁷ G. MAUJEAN, « Comment un faux tweet a fait plonger Wall Street », *Les Échos*, 24 avril 2013, en ligne à URL : <https://www.lesechos.fr/2013/04/comment-un-faux-tweet-a-fait-plonger-wall-street-338456> consulté en ligne le 15 février 2022.

¹¹⁹⁸ C. FERAL-SCHUHL, « Des droits de la personne renforcés », in *Les données personnelles*, Praxis Cyberdroit, Dalloz, 2020-2021.

¹¹⁹⁹ L'article 7 du RGPD définit le responsable de traitement comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

¹²⁰⁰ Fiche d'orientation, *Profilage*, Dalloz, septembre 2022. Voir aussi « Le profiling à la française », *Droit pénal*, Dalloz, décembre 2018, entretien avec Elen Duidard.

¹²⁰¹ L'article 4.4 du RGPD prévoit que profilage et la mise en place de décisions individuelles automatisées sont soumis à des obligations spécifiques. Voir aussi « Reconnaissance faciale : enjeux présents et à venir, Libertés fondamentales et droits de l'homme », Dalloz 2023, en ligne à URL : <https://actu.dalloz-etudiant.fr/a-la-une/article/reconnaissance-faciale-enjeux-presents-et-a-venir/h/2643e58cbb39b188739ccd9e58b0b3ef.html> consulté le 19 novembre 2023.

traitement est illicite *ab initio* ou devenu tel, en raison du retrait du consentement par exemple¹²⁰². Pour ce qui est de l'article 21, il offre la prérogative la plus exorbitante en matière de profilage, avec la faculté de pouvoir s'opposer aux profilages ayant pour finalité la prospection, prévue aux articles 21, § 2 et suivants. Une personne peut exercer son droit d'effacement par divers moyens : adresse électronique, formulaire, bouton de téléchargement ou par courrier. La personne concernée doit préciser quelles sont les données qu'elle souhaite effacer, car l'exercice de ce droit n'entraîne pas la suppression définitive et simple de toutes les données qui sont détenues par l'organisme.

Par ailleurs, l'article 35 du règlement impose expressément une analyse d'impact relative à la protection des données à caractère personnel en cas de profilage sur la base duquel « sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire »¹²⁰³.

Pour le Contrôleur européen de la protection des données, la législation européenne relative à la protection des données a justement été élaborée pour protéger les valeurs et les droits fondamentaux des Européens, dont le droit au respect à la vie privée. Dans ce contexte, les principes en matière de protection des données à caractère personnel, notamment la transparence, la proportionnalité et la limitation de la finalité, la reddition de comptes et le respect de la vie privée, dès la conception et par défaut, constituent les principes directeurs d'un droit moderne. Ce dernier serait animé par l'idée que la technologie doit servir la promotion de l'innovation et la sauvegarde des droits fondamentaux sans que la technologie ait à dicter ces valeurs et ces droits. Seul un traitement responsable des données massives peut apporter des avantages et des gains d'efficacité concrets à la société et aux individus ; sans cela, le traitement d'énormes quantités de données sur les droits et les libertés des personnes concernées suscitera toujours d'énormes inquiétudes au regard de la garantie du droit au respect de la vie privée¹²⁰⁴.

Sous-section 2 – Le profilage face aux règles régissant le traitement des données personnelles des passagers aériens

La prévention du profilage illicite est une préoccupation pour les juristes, car cette opération soulève divers problèmes liés aux droits fondamentaux. Ces pratiques peuvent, en effet,

¹²⁰² CNIL, « Le droit de l'effacement : supprimer vos données en ligne », Comprendre mes droits, 2022, en ligne à URL : <https://www.cnil.fr/fr/le-droit-leffacement-supprimer-vos-donnees-en-ligne> consulté le 24 janvier 2023.

¹²⁰³ Article 35, § 3, a, Règlement général sur la protection des données.

¹²⁰⁴ Avis du CEPD, 19 nov. 2015, «Relever les défis des données massives : Un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition de comptes».

enfreindre des principes juridiques bien établis tels que la non-discrimination et l'égalité mais aussi le droit au respect de la vie privée et à la protection des données à caractère personnel. C'est dans ce dernier cas que des interrogations subsistent sur l'efficacité de telles opérations ainsi que de leurs éventuelles conséquences négatives sur les relations entre les autorités publiques, notamment celles chargées de la gestion des frontières, et les citoyens qu'elles desservent.

§ 1 – Le profilage des données personnelles des passagers aériens dans les aéroports

Selon les données de l'Association Internationale du Transport Aérien (IATA), le nombre de passagers aériens dans le monde a atteint environ 4,5 milliards en 2023. En Europe, ce chiffre est approximativement de 1,2 milliard de passagers pour l'année 2023¹²⁰⁵. En France, cette activité aérienne concerne 102 compagnies aériennes autorisées à effectuer des vols, conformément à la liste des transporteurs aériens français. Cette liste recense les sociétés disposant d'un certificat de transporteur aérien et d'une licence d'exploitation valides¹²⁰⁶. Avec l'augmentation continue du nombre de passagers aériens à travers le monde, les États accumulent un volume de données de plus en plus important concernant les passagers.

En France, les autorités disposent des différents types de fichiers de données. Le fichier PNR ne peut être consulté directement par les autorités qui l'utilisent¹²⁰⁷. En effet, chaque service doit présenter une demande à l'UIP, qui peut être validée ou refusée par celui-ci, garantissant ainsi la protection des données des passagers aériens. Les fichiers de police et les dossier passagers ont des objectifs similaires ; toutefois, la raison de la collecte des données est bien différente dans chaque cas puisque chaque passager aérien voit ses données à caractère personnel collectées par la simple réalisation d'une réservation. Dans ce cas, la collecte systématique des données des passagers aériens n'est pas comparable avec une collecte ponctuelle d'informations sur des individus soupçonnés ou condamnés¹²⁰⁸.

La collecte d'informations sur les passagers aériens est devenue omniprésente dans les aéroports et la nécessité de protéger ces données à caractère personnel l'est devenue tout autant. Ces données de passagers sont susceptibles d'être transmises à un très grand nombre

¹²⁰⁵ IATA Sustainability and Economics, Tourism Economics, September 2023 release in IATA, *Global outlook for air transport, a local sweet spot*, décembre 2023.

¹²⁰⁶ DGAC, « Liste des transporteurs aériens français », 31 décembre 2023, en ligne à URL : https://www.ecologie.gouv.fr/sites/default/files/documents/Liste_compagnies_aeriennes_francaises_autorisees.pdf consulté le 26 août 2024.

¹²⁰⁷ Code de la sécurité intérieure, notamment ses articles L.232-1 à L. 232-7-1 et R.232-1 à R.232-22.

¹²⁰⁸ L. ARCHAMBAULT, B. TIGAUD, « La directive PNR et son articulation avec le RGPD : l'instauration d'un fichier de données des passagers aériens, outil efficace de la lutte contre le terrorisme et respectueux des données personnelles », *Gazette du Palais*, n° 6, LGDJ, 12 février 2019.

de destinataires, comme les autorités publiques ; cet état de fait augmente considérablement les risques de violations et la probabilité qu'elles fassent l'objet d'interventions malveillantes. Dans ce contexte, les données personnelles des passagers aériens apparaissent particulièrement vulnérables. Par ailleurs, l'interconnexion de bases de données à travers la mise en place de dispositifs censés offrir une expérience de voyage plus fluide et confortable aux voyageurs, notamment au moment de leur contrôle, ne rend que plus complexe la mission dévolue aux transporteurs aériens, lorsqu'il s'agit de la protection des données collectées¹²⁰⁹.

En effet, l'impératif de protection de « la confidentialité, l'intégrité et la disponibilité des systèmes et données informatiques et de communications critiques utilisées aux fins de l'aviation civile » est aujourd'hui un principe. Conséquemment, il invite tout transporteur à prendre les mesures nécessaires pour préserver les droits et libertés des personnes faisant l'objet d'une collecte mais cette protection ne saurait éloigner toutes les menaces qui pèsent sur ces données. Les multiples attaques dont ont fait l'objet les transporteurs aériens en témoignent, en produisant une fuite des données personnelles des voyageurs¹²¹⁰.

Dès lors qu'il implique la collecte et l'utilisation à court, moyen ou long terme de toutes les informations touchant à l'individu, le profilage est vu comme un mécanisme intrusif. Le nombre de données captables est ce qui caractérise l'intrusion. En effet, cette technique aboutit à nier l'essence même de l'individu en le réduisant à une catégorie sur la base de calculs statistiques, sans avoir égard à sa possibilité de changer. Ainsi, la moindre donnée personnelle est susceptible de renseigner sur les agissements futurs de l'individu qu'elle touche. Avant de valider cette tendance, le préalable est de déterminer le degré de prédictibilité de la donnée étudiée et ce n'est que si la valeur prédictive est élevée que la prise en compte des prévisions peut être considérée comme pertinente. Ces critiques relèvent, en fin de compte, un état de fait qui soulève des défis pour la société civile avec la mise à l'épreuve des libertés publiques devant les enjeux sécuritaires qui se posent¹²¹¹.

Le contrôleur européen pour la protection des données critique, en particulier, le profilage qui consiste à bâtir des hypothèses de risque à partir de données personnelles ne caractérisant pas une infraction¹²¹². En effet, l'élaboration de modèles de déplacements et de comportements

¹²⁰⁹ S. PARIER, « L'action de groupe et le RGPD en matière de transport aérien », *Activités touristiques – Données personnelles*, *Juris tourisme*, n° 215, p.44, Dalloz, 2019.

¹²¹⁰ Ibidem

¹²¹¹ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.

¹²¹² Avis du CEPD, 9 déc. 2011, sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers

conduit à fonder des décisions à l'encontre d'individus qui auront ensuite le plus grand mal à se défendre contre ces décisions. Le profilage doit être appréhendé comme un processus impliquant plusieurs techniques, d'abord la captation des informations et ensuite l'analyse de ces informations.

Le profilage s'effectue à partir de l'analyse des autres données PNR, le nom permettant dans un second temps de relier cette analyse à un individu. Par ailleurs, étant donné que le nom est l'une des données les moins fiables du système PNR, la consultation des données APIS et des documents de voyage est le moyen le plus pertinent pour s'assurer de l'identité exacte d'une personne¹²¹³. Les experts en sécurité attirent l'attention sur le fait que les autres systèmes d'identification sont particulièrement utiles pour identifier une personne avec certitude et déclencher des mesures, comme une arrestation, lorsque cette personne attire déjà l'attention des services de sécurité. Toutefois, la particularité des données PNR réside ailleurs : elles sont aussi utiles pour détecter des personnes non connues des services de sécurité mais dont certains comportements peuvent être révélateurs d'un risque criminogène¹²¹⁴.

L'analyse des données PNR permet de déterminer les hypothèses de risques de manière fiable et ciblée et de mettre ainsi en place les contrôles et surveillances nécessaires, selon les experts en contre-terrorisme. D'ailleurs, en matière douanière, le sous-directeur de la direction des douanes¹²¹⁵ a expliqué que le ciblage des contrôles est devenu un outil indispensable et décisif dans l'efficacité des services. Par exemple, en matière de stupéfiants, 60% à 80% des saisies dans les aéroports sont effectuées à la suite de ciblage¹²¹⁶. D'après certains tests, le taux de résultat des contrôles ciblés est huit fois supérieur au taux de résultat des contrôles aléatoires. Bien que la plus-value des données soit difficile à évaluer, elle n'en demeure pas moins efficace.

Comme l'explique l'ancien directeur central du renseignement intérieur français, le terrorisme international actuel repose sur des individus relativement isolés agissant en réseau tandis que

passagers (données PNR) au ministère américain de la sécurité intérieure : JOUE n° C 35, 9 févr. 2012, p. 16, §10.

¹²¹³ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.

¹²¹⁴ S. PEYROU, « De l'accord PNR à Prism, bilan et perspectives sur les malentendus transatlantiques : lutte anti-terroriste versus protection des données personnelles », *GDR ELSJ*, 11 septembre 2013, en ligne à URL : <https://www.gdr-elsj.eu/2013/09/11/droits-fondamentaux/de-laccord-pnr-a-prism-bilan-et-perspectives-sur-les-malentendus-transatlantiques-lutte-anti-terroriste-versus-protection-des-donnees-personnelles/> consulté le 19 novembre 2023.

¹²¹⁵ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016

¹²¹⁶ Ibidem

par le passé, le terrorisme reposait davantage sur un support étatique¹²¹⁷. Le terrorisme a donc connu une évolution qui implique, pour les États, de réaliser une détection précoce en vue de prévenir et d'évaluer le risque et la dangerosité. Ainsi, l'analyse des données PNR permet d'identifier le lieu et l'environnement d'une personne afin de l'empêcher de passer à l'acte, car ces données, lorsqu'elles sont prises de manière cumulatives, représentent des signaux d'alarme significatifs. Le directeur du renseignement a souligné, par ailleurs, qu'en matière de renseignement, une donnée prise isolément est rarement décisive mais vient plutôt compléter une panoplie d'autres données¹²¹⁸. Pour cette raison l'évaluation de la plus-value propre dans la lutte contre le terrorisme n'est pas sans difficulté. Il s'agit là d'un argument pour ceux qui émettent des critiques contre les règles PNR européennes.

En effet, un individu qui passe une frontière s'expose toujours à des contrôles exorbitants par rapport à ceux auxquels il est exposé sur le territoire d'un État de droit¹²¹⁹. Le développement des systèmes PNR peut, dès lors, apparaître comme n'étant pas d'une nature si différente des contrôles applicables à ce jour aux voyageurs internationaux, comme le contrôle d'identité. Cela n'est que la traduction du principe de souveraineté des États¹²²⁰.

Par ailleurs, il semblerait que l'utilité des données n'est pas suffisante en elle-même pour justifier ce système. Le principe de la proportionnalité sous-entend de mettre en balance les gains pour la sécurité et les sacrifices consentis au détriment du respect des droits fondamentaux. Les systèmes PNR peuvent être comparés à des « filets dérivants » capturant de nombreuses données relatives à des citoyens ordinaires. Ils permettent, d'une part, de détecter des activités terroristes ou criminelles et, d'autre part, de conserver ces données pendant plusieurs années en cas de besoin. Ce système est distinct de celui des fichiers de police traditionnels qui ont pour objet d'accumuler des données sur des personnes déjà connues des services. Ainsi, le reproche principal adressé à la collecte des données de passagers aériens est le suivant : les collectes indifférenciées font de chaque utilisateur un potentiel suspect¹²²¹.

Pour une partie de la doctrine, la démarche « proactive » du système PNR, puisqu'il vise à évaluer le risque que peuvent représenter certains passagers, aboutit à un profilage

¹²¹⁷ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.

¹²¹⁸ S. SUTOUR, Y. DETRAIGNE, « Rapport n° 401 : La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives », *Commission des lois*, Sénat, 13 mai 2009

¹²¹⁹ M-C. GRANGER, « Existe-t-il un droit fondamental à la sécurité ? », *Revue de Sciences Criminelles*, 2009, p. 273.

¹²²⁰ S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.

¹²²¹ Ibidem.

indifférencié de millions de citoyens. En cela, ce système peut porter atteinte au droit fondamental à la protection des données à caractère personnel tel que défendu par l'article 8 de la Charte des droits fondamentaux¹²²². L'apport de la Cour de justice, depuis l'arrêt *Digital Rights Ireland Ltd (C-293/12)* du 8 avril 2014, est ici essentiel, car les juges de Luxembourg ont censuré le stockage de masse de données et imposé un certain nombre de garde-fous. Ces derniers peuvent s'imposer dans les textes de loi comme la directive sur les dossiers passagers.

La technique du profilage semble toutefois faire son chemin chez les élites politiques européennes malgré les limites que tentent de mettre en place les juridictions européennes. En effet, lorsque les dirigeants européens sont interrogés sur leur vision des libertés publiques, leur réponse tend souvent à vouloir se distinguer des États rivaux ou plus franchement autoritaires, comme la Russie ou la Chine par exemple, afin démontrer leur supposée supériorité morale tout en rejetant immédiatement les critiques « droits-de-l'homme »¹²²³. Le traçage numérique est considéré comme ne faisant pas partie de la « culture française », selon un ancien ministre de l'Intérieur français lorsque des journalistes l'ont interrogé sur les pratiques du régime chinois au début de la pandémie de Covid-19¹²²⁴. Si la Chine est encore vue comme un repoussoir dans les discours, sa domination en matière de surveillance en a fait un partenaire important, ses entreprises remportant ainsi régulièrement la majorité des marchés publics français. Par exemple, en juillet 2020, le ministère de l'Intérieur français a passé une commande de 15 millions d'euros pour l'achat de 30 000 nouvelles caméras-piétons destinées à filmer les interventions des forces de l'ordre, après un appel d'offres que l'entreprise chinoise Hikvision a remporté¹²²⁵.

Les autorités publiques françaises semblent considérer que combiné aux dizaines de milliers de caméras de vidéosurveillance installées sur les autoroutes, le profilage permet la maîtrise de soi et donc une limitation des comportements non-civilisés à l'instar du modèle social de la Chine avec son « score de crédit social » qui vise à mettre en place un système national de réputation des citoyens et de construire ainsi une société de surveillance où les algorithmes et l'intelligence artificielle sont les piliers d'une gouvernance qui distribue, via les technologies,

¹²²² Article 8, Charte des droits fondamentaux.

¹²²³ F. TREGUER, « Surveillance numérique », in *Le Nouveau Monde : Tableau de la France néolibérale*, Editions Amsterdam, 2021.

¹²²⁴ Ibidem.

¹²²⁵ Ibid.

les bons et mauvais points aux citoyens constamment surveillés¹²²⁶. Certains membres des forces de l'ordre y voient même un moyen de « mettre fin à des années de polémiques sur le contrôle au faciès, puisque le contrôle d'identité serait permanent et général », mais aussi « invisible »¹²²⁷. Les promoteurs français de ces nouvelles technologies de profilage misent sur les Jeux olympiques de 2024, un événement sportif majeur et donc un marché public lucratif, à propos desquels les inquiétudes sécuritaires sont énormes, pour s'assurer de l'acceptation sociale de la reconnaissance faciale en espérant que les craintes sur les questions de surveillance soient éclipsées par le caractère festif et rassembleur de cet événement sportif.

Le ministère de l'Intérieur français semble adopter une approche à long-terme sur le sujet du profilage. Au mois de novembre 2020, le gouvernement a discrètement publié le Livre blanc de la sécurité intérieure alors que le pays était en pleine mobilisation contre la proposition de loi dite « Sécurité globale » et connaissait des violences policières. Ce texte prévoit toute une panoplie de techniques sécuritaire comme l'identification biométrique par reconnaissance faciale, le son de la voix ou les odeurs corporelles, des centres de commandement nourris aux Big Data afin de procéder à « l'analyse des données du passé comme outil de rétrocontrôle et d'aide à la décision » en utilisant l'intelligence artificielle « pour faire face au volume croissant d'informations », ou encore à la multiplication des drones de surveillance¹²²⁸. Ce Livre blanc propose de consacrer 1 % du PIB aux missions de sécurité intérieure, à l'horizon 2030, afin de « porter le ministère de l'Intérieur à la frontière technologique », soit une augmentation budgétaire de 30 % sur la décennie.

§ 2 – L'encadrement juridique du profilage des données personnelles des passagers aériens

Contrairement au RGPD qui prévoit explicitement le profilage, la directive relative à l'utilisation des données des dossiers passagers¹²²⁹ n'évoque que le traitement automatisé de celles-ci. Cette notion y est mentionnée neuf fois. Dès le préambule, la directive énonce, dans l'hypothèse d'un traitement de données PNR qu'aucune décision qui « produit des effets juridiques préjudiciables à une personne ou l'affecte de manière significative ne devrait être

¹²²⁶ B. PEDROLETTI, « En Chine, le « crédit social » des citoyens fait passer les devoirs avant les droits », *Le Monde*, 16 janvier 2020 en ligne à URL : https://www.lemonde.fr/idees/article/2020/01/16/le-credit-social-les-devoirs-avant-les-droits_6026047_3232.html consulté le 27 juin 2023.

¹²²⁷ F. TREGUER, « Surveillance numérique », *Le Nouveau Monde : Tableau de la France néolibérale*, Editions Amsterdam, 2021.

¹²²⁸ Ministère de l'Intérieur, « Le livre blanc de la sécurité intérieure », 2020.

¹²²⁹ 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.

prise » afin de ne pas aller à l'encontre du « droit à la protection des données à caractère personnel et du droit à la non-discrimination »¹²³⁰.

La terminologie utilisée n'est pas sans rappeler la logique présente dans le RGPD qui veille à ce que le profilage ou le traitement automatisé des données à caractère personnel ne produise pas des effets allant à l'encontre des dispositions de la Charte des droits fondamentaux de l'Union européenne, notamment ses articles 8 et 21 condamnant toute décision discriminante fondée sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle¹²³¹.

Le profilage, sans être mentionné explicitement, est énoncé à l'article 6, paragraphe 2, a) de la directive visant le traitement des données PNR à l'égard de critères préétablis¹²³². Les données PNR sont traitées essentiellement à des fins prédictives en utilisant des algorithmes permettant d'identifier les passagers qui pourraient être impliqués dans des infractions terroristes ou dans des crimes organisés. Dans ce contexte, les données personnelles des passagers aériens transférées par les transporteurs aériens sont recueillies par l'UIP de l'État membre. Dans le cas d'un traitement des données à des fins prédictives, l'UIP réalise en substance une activité de profilage. Cette opération est susceptible d'entraîner des conséquences juridiques non négligeables sur les individus identifiés par l'algorithme en question. C'est pourquoi un tel traitement de données requiert un encadrement juridique précis « en ce qui concerne tant les modalités de sa réalisation que les garanties qui doivent l'entourer »¹²³³. La CJUE a relevé, au point 172 de l'avis 1/15 déjà mentionné, l'étendue des données traitées dans ces types d'analyses avec des modèles et des critères préétablis appliqués, mettant ainsi en péril les droits consacrés aux articles 7 et 8 de la Charte¹²³⁴, à savoir le droit à la vie privée et la protection des données personnelles.

L'article 6, paragraphe 4, deuxième phrase de la directive sur les dossiers passagers énonce que les critères préétablis au regard desquels est réalisée l'évaluation préalable prévue à l'article 6, paragraphe 3, b) de cette directive doivent être « ciblés, proportionnés et spécifiques ». La première de ces exigences renvoie à l'objectif visé par l'évaluation préalable

¹²³⁰ Directive (UE) PNR, Préambule, §20.

¹²³¹ Charte des droits fondamentaux de l'Union européenne, articles 8 et 21.

¹²³² Directive (UE) PNR, article 6, paragraphe 2, sous a).

¹²³³ CJUE, Conclusions de l'avocat Général M. Giovanni Pitruzzella, Affaire C-817/19, Ligue des droits humains contre Conseil des ministres, 27 janvier 2022.

¹²³⁴ CJUE, 26 juillet 2017, avis 1/15.

prévue au paragraphe 2, a) de cette disposition, à savoir l'identification des individus pour lesquels est requis un examen plus approfondi par les autorités compétentes, et répond ainsi à la nécessité, exposée par la Cour dans l'avis 1/15, que les critères utilisés parviennent à « cibler » les individus à l'égard desquels pourrait peser un « soupçon raisonnable » de participation à des infractions terroristes ou de crimes organisés¹²³⁵. Ce « ciblage » implique l'application de critères d'évaluation abstraits. Une recommandation de 2021 sur le profilage encourageait d'utiliser des filtres de données des dossiers passagers aux profils établis dans le but de repérer les passagers qui y répondent et à qui les autorités compétentes appliqueraient un contrôle plus approfondi¹²³⁶.

En revanche, la directive européenne sur les dossiers passagers interdit le profilage individuel de tous les passagers aériens dont les données sont analysées, par exemple en associant à chacun d'eux une catégorie de risque sur une échelle prédéfinie, sous peine de violer tant l'article 6, paragraphe 4 de cette directive que les limites tracées par les juges de Luxembourg au traitement automatisé des données personnelles des passagers aériens dans l'avis 1/15¹²³⁷.

La directive PNR interdit expressément le profilage discriminatoire à l'article 6, paragraphe 4, première phrase qui prévoit que l'évaluation préalable au regard de critères préétablis au titre du paragraphe 3, point b) de ce même article « est réalisée de façon non discriminatoire ». Si la troisième phrase de l'article 6, paragraphe 4, considère que lesdits critères « ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle », l'interdiction générale du profilage discriminatoire est appelé à s'entendre au regard de tous les motifs de discrimination de l'article 21 de la Charte, même ceux qui ne sont pas expressément mentionnés¹²³⁸.

L'article 6, paragraphe 3, b) de la directive PNR et le système de garanties qui entoure le traitement automatisé des données PNR prévu aussi par cette directive¹²³⁹ impliquent que le fonctionnement des algorithmes utilisés dans le cadre de l'analyse doit être transparent et le résultat de leur mise en œuvre traçable. Cette transparence exigée n'implique pas que les profils identifiés soient rendus publics ; toutefois, cette exigence requiert que soit assuré le caractère identifiable d'une telle prise de décision bâtie sur des algorithmes. La première raison de cette logique est l'exigence selon laquelle les critères sur lesquels cette analyse doit

¹²³⁵ Ibidem

¹²³⁶ CJUE, Conclusions de l'avocat Général M. Giovanni Pitruzzella, op.cit.

¹²³⁷ Ibidem

¹²³⁸ Ibid.

¹²³⁹ Ibid.

être effectuée doivent être « préétablis », ce qui signifie qu'ils ne peuvent être modifiés sans intervention humaine et s'oppose donc à l'utilisation de technologies d'intelligence artificielle comme celle du « machine learning »¹²⁴⁰, qui, tout en pouvant présenter un degré de précision plus élevé, sont difficiles à interpréter, même pour les opérateurs qui ont effectué le traitement automatisé. La deuxième raison est la garantie prévue à l'article 6, paragraphes 5 et 6 de la directive PNR énonçant que toute réponse positive obtenue à la suite du traitement automatisé des données des dossiers passagers effectué en vertu du paragraphe 2, point a) dudit article sera réexaminée individuellement par les moyens non automatisés. Pour être efficaces, il est nécessaire – au regard de l'analyse visée à l'article 6, paragraphe 3, point b) de la directive PNR – qu'il soit possible de comprendre la raison pour laquelle le programme est arrivé à une telle concordance, ce qui ne peut être garanti en pratique lorsque des systèmes d'auto-apprentissage sont utilisés¹²⁴¹.

Il en est de même du contrôle de la licéité de cette analyse, y compris au regard du caractère non-discriminatoire des résultats obtenus, dont sont investis le délégué à la protection des données et l'autorité nationale de contrôle, respectivement en vertu de l'article 6, paragraphe 7 et l'article 15, paragraphe 3, b) de la directive¹²⁴². La transparence dans le fonctionnement des algorithmes utilisés est également une condition nécessaire afin de permettre aux individus concernés d'exercer, le cas échéant, leur droit de réclamation ainsi que leur droit à un recours juridictionnel effectif¹²⁴³.

Plusieurs garanties entourent le traitement automatisé des données des passagers aériens dans le cadre de l'évaluation préalable au titre de l'article 6, paragraphe 2, a) de la directive PNR, répondant par la même occasion aux exigences énoncées par les juges de Luxembourg dans l'avis 1/15, dont l'actualisation à intervalles réguliers des critères préétablis au regard desquels doit être effectuée l'évaluation préalable visée à l'article 6, paragraphe 3, sous b) de cette directive (article 6, paragraphe 4, troisième phrase de la directive PNR ; avis 1/15, point 174), l'interdiction de traitement sur la base de critères préétablis discriminatoires (article 6, paragraphe 4, première et quatrième phrase de la directive PNR ; avis 1/15, point 172), le réexamen par des moyens non automatisés de toute concordance positive obtenue à la suite du traitement automatisé des données PNR (article 6, paragraphes 5 et 6 de la directive PNR ; avis 1/15, point 173) et le contrôle de la licéité de ce traitement par le délégué à la protection

¹²⁴⁰ Le « machine learning » est une technique de programmation informatique qui utilise des probabilités statistiques pour donner aux ordinateurs la capacité d'apprendre par eux-mêmes sans programmation explicite.

¹²⁴¹ CJUE, Conclusions de l'avocat Général M. Giovanni Pitruzzella, Affaire C-817/19, Ligue des droits humains contre Conseil des ministres, 27 janvier 2022.

¹²⁴² Ibidem.

¹²⁴³ Ibid.

des données et par l'autorité nationale de contrôle (article 6, paragraphe 7, et article 15, paragraphe 3, sous b) de la directive PNR)¹²⁴⁴. À cet égard, le contrôle effectué par une autorité indépendante semble primordial, comme l'énonce l'article 15 de la directive PNR, et doit porter sur tout aspect inhérent au traitement automatisé des données des dossiers passagers, incluant l'identification des données utilisées aux fins de la confrontation prévue à l'article 6, paragraphe 3, sous a) de cette directive et l'élaboration des critères préétablis appliqués aux fins de l'analyse au titre de l'article 6, paragraphe 3, sous b), de ladite directive et qu'il puisse être exercé tant *ex ante* que *ex post*¹²⁴⁵.

Ces garanties sont appelées à être appliquées de manière transversale aux deux types d'analyse évoqués à l'article 6, paragraphe 3 de la directive sur les dossiers passagers, bien que les termes dans lesquels elles sont formulées peuvent être équivoques. En effet, l'article 6, paragraphe 4, première phrase de la directive PNR réitère l'exigence du respect du principe de non-discrimination seulement par rapport à l'évaluation préalable réalisée au regard de critères préétablis, l'exigence susmentionnée s'impose dans toute étape du processus du traitement des données des dossiers passagers. Elle est donc également imposée lorsque ces critères sont confrontés aux bases de données pertinentes dans le cadre de l'évaluation préalable au sens de l'article 6, paragraphe 3, sous a) de cette directive¹²⁴⁶.

La même logique sous-tend l'exigence selon laquelle les critères préétablis utilisés dans le cadre de l'analyse visée à l'article 6, paragraphe 3, sous b) de la directive doivent être fiables, mis à jour et être compris comme visant aussi les données contenues dans les bases de données utilisées aux fins de la confrontation prévue à l'article, paragraphe 3, sous a) de ladite directive. Toutes les garanties applicables aux traitements automatisés de données personnelles évoquées par la directive police sont également applicables dans le cadre de la directive PNR. Ainsi, les analyses automatisées opérées dans le cadre de ladite directive doivent être considérées comme entrant dans le champ d'application de la directive police¹²⁴⁷.

Enfin, une garantie évoquée à l'article 7, paragraphe 6 de la directive PNR prévoit, d'une part, l'interdiction de fonder tout processus de décision exclusivement sur les résultats du traitement des données PNR et, d'autre part, l'interdiction de discrimination dans le traitement et l'utilisation des données susmentionnées. Cette disposition prévoit que « les autorités compétentes ne peuvent prendre aucune décision produisant des effets juridiques

¹²⁴⁴ Ibid.

¹²⁴⁵ Ibid.

¹²⁴⁶ Ibid.

¹²⁴⁷ Ibid.

préjudiciables à une personne ou l'affectant de manière significative sur la seule base du traitement automatisé de données PNR » et que ces décisions « ne peuvent pas être fondées sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle »¹²⁴⁸. Pour garantir la sécurité des données des passagers aériens, l'article 6, paragraphe 8 de la directive prévoit que le stockage, le traitement et l'analyse de ces données par les UIP sont effectués exclusivement dans un ou des endroits sécurisés situés sur le territoire des États membres¹²⁴⁹.

Cette volonté d'anticiper les menaces, par la technique du profilage, s'inscrit dans l'action de l'Union européenne face au terrorisme. Il constitue une priorité pour les États membres européens qui coopèrent de différentes manières pour prévenir les attentats terroristes afin d'assurer la sécurité des citoyens européens. En effet, les États européens ont fait face à une série d'attentats perpétrés dans les capitales européennes, ces dix dernières années. Par ailleurs, en 2015, les États membres ont publié une déclaration commune destinée à orienter les travaux de l'Union européenne dans trois domaines : la garantie de la sécurité des citoyens, la prévention de la radicalisation et la protection des valeurs européennes et la coopération avec les partenaires à l'échelon international¹²⁵⁰.

Le profilage s'inscrit à la fois dans une logique de prévention de la radicalisation, à travers l'utilisation des technologies, et une politique d'échange d'informations entre les services répressifs afin de lutter efficacement contre le terrorisme. Il est visé une meilleure coordination entre les États membres pour lutter contre les infractions terroristes mais aussi l'entrée des combattants étrangers sur le territoire de l'Union européenne. Le droit de l'Union définit ces infractions comme des actes commis dans le but de gravement intimider une population, contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque ou de gravement déstabiliser ou détruire les structures politiques, constitutionnelles, économiques ou sociales fondamentales d'un pays ou d'une organisation internationale¹²⁵¹.

La directive relative aux données des dossiers passagers qui régit le transfert et le traitement des données à caractère personnel fournies par les passagers aériens met en avant le profilage

¹²⁴⁸ Directive (UE) PNR, Article 7, paragraphe 6.

¹²⁴⁹ Directive (UE) PNR, Article 6, paragraphe 8.

¹²⁵⁰ Conseil européen, « Déclaration des membres du Conseil européen sur la lutte contre le terrorisme », *Communiqués de presse*, 12 février 2015, en ligne à URL : <https://www.consilium.europa.eu/fr/press/press-releases/2015/02/12/european-council-statement-fight-against-terrorism/> consulté en ligne le 25 février 2022.

¹²⁵¹ Conseil européen, « L'action de l'UE face au terrorisme », *Politiques*, 15 décembre 2022, en ligne à URL : <https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/> consulté en ligne le 15 février 2022.

dans ce but, puisqu'elle considère dans son préambule que « l'utilisation effective des données PNR, par exemple la confrontation des données PNR à diverses bases de données de personnes ou d'objets recherchés, est nécessaire 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 donc pour renforcer la sécurité intérieure, pour rassembler des preuves et, le cas échéant, pour trouver les complices de criminels et démanteler des réseaux criminels »¹²⁵². Dans le cadre de ces missions, les données des dossiers passagers peuvent être utilisées de plusieurs sortes : pour la mise au point de ces critères de risque ; aux fins de l'évaluation du risque que représentent les passagers avant leur départ ou avant leur arrivée au regard de critères de risque arrêtés ; aux fins de l'identification d'individus donnés dans le cadre d'enquêtes ou de poursuites singulières.

Pour protéger les droits fondamentaux en matière de protection des données à caractère personnel, le droit au respect de la vie privée et le droit à la non-discrimination, la directive prévoit une série de limites en ce qui concerne le traitement, le transfert et la conservation des données des passagers aériens : celles-ci ne peuvent être conservées que pendant une période de 5 ans et doivent être rendues anonymes après une période de 6 mois de manière à ce que la personne concernée ne soit plus immédiatement identifiable ; les États membres sont tenus de mettre en place une unité d'informations passagers chargée de la gestion et de la protection des données ; cette unité doit comprendre un délégué à la protection des données ; la directive interdit la collecte et l'utilisation de données sensibles ; le traitement automatisé de données des passagers aériens ne peut constituer la seule base pour adopter une décision susceptible de produire des effets juridiques préjudiciables ou d'affecter gravement une personne ; les États membres doivent veiller à ce que les passagers soient clairement informés de la collecte de données personnelles de passagers et de leurs droits à cet égard ; le transfert de données des dossiers passagers à des pays tiers ne peut avoir lieu que dans des cas très limités et au cas par cas.

¹²⁵² Considérant 6), 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.

Chapitre 2 – L’affaiblissement de la protection juridique des dossiers passagers par le rôle des acteurs privés dans les aéroports

Les avions transportent aujourd’hui un grand nombre de voyageurs et les aéroports sont souvent décrits comme des frontières intérieures où les étrangers convergent et se dispersent. L’aéroport est aussi un lieu où l’autorité de l’État s’exerce pour maintenir la sécurité. Ainsi, les autorités chargées du contrôle des frontières s’efforcent d’obtenir, de manière efficace, des informations sur l’identification des voyageurs, de leurs bagages et du sens de leur voyage dans le cadre de la lutte contre la criminalité en tout genre, en particulier le terrorisme et les crimes transnationaux¹²⁵³.

Les menaces qui pèsent sur les aéroports impliquent de distinguer les notions de sécurité et de sûreté aérienne. La première requiert des précautions techniques prises pour éviter les accidents aéronautiques dont les causes seraient involontaires¹²⁵⁴. Cette notion regroupe les règles de construction et d’utilisation des avions. Plus généralement, elle désigne l’ensemble des moyens mis en place pour prévenir les accidents. La sécurité renvoie à une norme ou un système de prévention contre les défaillances structurelles, mécaniques ou météorologiques. Une réglementation stricte permet la réalisation de l’objectif de sécurité à travers des normes de fabrication, d’utilisation et d’entretien des aéronefs ainsi que de critères rigoureux de formation et de qualification du personnel technique et des commerciaux¹²⁵⁵.

La seconde notion, la sûreté aérienne, fait référence, en principe, à la liberté individuelle mais dans le secteur aéroportuaire, elle implique un ensemble de mesures adoptées dans le but de prévenir tout acte malveillant visant l’aéronef¹²⁵⁶. L’annexe 17 de l’Organisation de l’aviation civile internationale (OACI) la définit plus précisément comme la « combinaison des mesures ainsi que des moyens humains, matériels visant à protéger l’aviation civile contre les actes d’interventions illicites ». Les actes mal intentionnés renvoient aux tentatives de prise d’otages, d’agression, de sabotage ou de détournement.

¹²⁵³ C. R. HAN, R. MCGAURAN, H. NELEN, « API and PNR data in use for border control authorities », *Security Journal*, 2016.

¹²⁵⁴ H. PROTAR, *La sûreté aéroportuaire en France*, Mémoire de Master, Université Panthéon-Assas-Paris II, 2016.

¹²⁵⁵ Ibidem

¹²⁵⁶ Ibid.

Le développement de l'offre de service de tout type aux passagers n'a fait qu'augmenter la masse de données collectées sur les voyageurs. À titre d'illustration, le consommateur se voit de plus en plus proposer des offres de voyage à forfait combinant la vente de billet avec d'autres prestations comme la location d'un véhicule ou un hébergement. Ces prestations complémentaires requièrent la collecte de nouvelles données à caractère personnel. La collecte d'informations à caractère personnel est donc devenue omniprésente pour le passager aérien ; un phénomène qui appelle une meilleure protection de ces données susceptibles d'être transmises à un nombre important de destinataires. Ces données ont un caractère vulnérable ; plus elles sont transmises, plus la probabilité qu'elles fassent l'objet d'utilisations malveillantes s'accroît pouvant nuire à leur confidentialité et à leur protection.

Tout un arsenal juridique a donc été mis en place par le législateur européen, nous l'avons vu, afin de protéger cette masse de données des passagers aériens que l'activité des transporteurs aériens produit. Rappelons que le texte le plus connu à cet égard est la directive 2016/681 du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité. Ainsi, les règles s'accumulent pour encadrer une utilisation et une transmission des données personnelles des passagers aériens de plus en plus développées.

L'aéroport, en tant que lieu où transitent toutes ces données, implique de nouveaux enjeux pour les juristes. Les aéroports sont à la pointe de l'innovation et sont aujourd'hui appelés à faire face à un nombre de passagers qui augmente de façon exponentielle chaque année¹²⁵⁷. De nouveaux défis surgissent et les acteurs des aéroports s'adaptent, c'est le cas avec l'utilisation de l'internet des objets (*Internet of Thing*, IoT)¹²⁵⁸ qui intègre des appareils intelligents pour le bien-être des voyageurs et des employés. Ces « aéroports intelligents » permettent de fournir des services optimaux de manière fiable et durable en travaillant autour des enjeux de croissance, d'efficacité, de sûreté et de sécurité. Primordiale dans le contexte de la révolution numérique, la cybersécurité devient un investissement clé pour la sécurité aéroportuaire.

De nos jours, des personnes privées, transporteurs ou professionnels de la sécurité, interviennent dans le secteur aéroportuaire. Or, cette participation soulève des problématiques juridiques, plus précisément au regard de son encadrement par les autorités publiques et ses

¹²⁵⁷ G. LYKOU, A. ANAGNOSTOPOULOU, D. GRITZALIS, « Smart airport cybersecurity: threat mitigation and cyber resilience controls », *Sensors* (Basel), 21 décembre 2018.

¹²⁵⁸ B. BENHAMOU, « L'internet des objets. Défis technologiques, économiques et politiques », *Esprit*, n° 3-4, 2009, pp. 137-150.

conséquences sur les droits fondamentaux des passagers aériens. La privatisation des aéroports en Europe soulève dans ce contexte de multiples enjeux. En 2020, la privatisation d'Aéroports de Paris (ADP) a été suspendue avec la crise du coronavirus mais le Gouvernement français n'a, semble-t-il, jamais abandonné l'idée de vendre ses actifs publics¹²⁵⁹. Dès lors, outre un affaiblissement de la protection juridique des dossiers passagers par l'ingérence des acteurs privés dans le traitement des données aux frontières (Section 1), des interrogations naissent également quant au phénomène de privation des aéroports (Section 2).

Section 1 – L'ingérence contestée des acteurs privés dans le traitement des dossiers passagers aux frontières

Les attaques terroristes du 11 septembre 2001 ont conduit à un regain d'intérêt pour la sécurité des aéroports à travers le monde. Avant cette tragédie, les politiques gouvernementales ne permettaient pas d'assurer un niveau de sécurité sous-optimal. Le recours à des sociétés privées est devenu de plus en plus fréquent en vue de pallier les manques en la matière mais cette évolution soulève des défis en matière de protection des données à caractère personnel (Sous-section 1). Le système actuel de sécurité renforcée est sensiblement plus coûteux et doit être évalué en termes de rapport coût-efficacité par rapport à une approche public-privé (Sous-section 2). La protection juridique des dossiers passagers est dans ce contexte mise à mal par l'ingérence des personnes privées (transporteurs ou professionnels de la sécurité) dans le cadre de l'exercice des missions de maîtrise des frontières qu'ils partagent avec l'État. Cette participation soulève plusieurs interrogations juridiques notamment quant à ses conséquences sur les libertés publiques.

Sous-section 1 – La participation accrue des acteurs privés dans la gestion des aéroports

Bien que l'entrée et la sortie du territoire d'un État demeure un domaine régalien, les autorités publiques n'agissent plus seules pour contrôler les mouvements des populations. L'État mobilise des personnes privées, professionnels de la sécurité et transporteurs, qui interviennent de plus en plus à ses côtés. Bien que justifiée, cette implication soulève des questions juridiques, notamment vis-à-vis des libertés fondamentales ; d'autant plus que l'encadrement de ce phénomène par la puissance publique est récent.

¹²⁵⁹ Rédaction, « Aéroports de Paris : pas de référendum, mais un report de la privatisation », *France 24*, 12 mars 2020, en ligne à URL : <https://www.france24.com/fr/20200312-a%C3%A9roports-de-paris-pas-de-r%C3%A9f%C3%A9rendum-mais-un-report-de-la-privatisation> consulté le 22 avril 2023.

§ 1 – L'évolution de la place des personnes privées dans les aéroports

Depuis les années 1990, le milieu aéroportuaire français se distingue par une augmentation progressive de l'appel aux services privés dans le but de contrôler l'afflux des passagers et des marchandises. Avant cette date, l'État était le seul en charge de l'exécution des mesures de sûreté dans les aéroports et l'ensemble des inspections et des contrôles étaient sous la responsabilité des agences des services étatiques. Considérés comme des établissements publics, les aéroports étaient placés sous l'autorité du ministère chargé des transports et dirigés par la direction générale de l'aviation civile (DGAC), l'administration en charge de la préparation des normes, de la coordination avec les autres services et de la gestion des équipements. La gendarmerie des transports aériens (GTA) était chargée de l'inspection des personnes et des véhicules ayant autorisation à accéder aux zones réservées et à la protection des aéronefs. La police aux frontières (PAF) devait, quant à elle, procéder aux contrôles en zone publique via l'inspection par filtrage des passagers et des bagages en cabines (IFPBC) et réaliser la garde en zone ouverte. Enfin, le service des douanes avait pour mission d'inspecter les bagages en soute, le courrier et le fret¹²⁶⁰.

En 1989, pour la première fois, la législation française a explicitement externalisé des missions de sûreté à des intervenants privés ; toutefois, dans les faits, des activités dans ce milieu avaient déjà été externalisées par les autorités étatiques. Le recours systématique à des agents privés a donc commencé avec la loi du 10 juillet 1989 modifiant l'article L. 282-8 du Code de l'aviation civile pour qu'il prévoit que les agents privés puissent « procéder à la visite des bagages, du fret, des colis postaux, des aéronefs et des véhicules » après que le préfet et le procureur aient donné leur agrément et sous le contrôle d'un officier de la police judiciaire¹²⁶¹. Cette externalisation ne s'est pas faite sans obstacles ; les autorités publiques ont rencontré des difficultés à accepter cette transition. De plus, notons que les agents privés avaient reçu pour consigne de ne pas s'adresser directement aux passagers pendant le contrôle dans les aéroports¹²⁶².

Puis, la loi du 26 février 1996 relative aux transports a étendu les prérogatives des agents privés en autorisant ces derniers à procéder à la visite des personnes. L'article L. 282-8 du Code de l'aviation civile modifié, aujourd'hui abrogé, disposait ainsi : « En vue d'assurer préventivement la sûreté des vols, tant en régime intérieur qu'international, d'une part les

¹²⁶⁰ H. PROTAR, *La sûreté aéroportuaire en France*, Mémoire de Master, Université Panthéon-Assas-Paris II, 2016.

¹²⁶¹ Ibidem

¹²⁶² Ibid.

officiers de police judiciaire ainsi que, sur l'ordre et sous la responsabilité de ceux-ci, les agents de police judiciaire et les agents de police judiciaire adjoints mentionnés aux 1°, 1° bis et 1° ter de l'article 21 du code de procédure pénale et, d'autre part, les agents des douanes, peuvent procéder à la fouille et à la visite par tous moyens appropriés des personnes, des bagages, du fret, des colis postaux, des aéronefs et des véhicules pénétrant ou se trouvant dans les zones non librement accessibles au public des aéroports et de leurs dépendances, ou sortant de celles-ci. Sont également habilités à procéder à ces fouilles et visites, sous le contrôle des officiers de police judiciaire ou des agents des douanes, les agents de nationalité française ou ressortissants d'un État membre de l'Union européenne désignés par les entreprises de transport aérien, les exploitants d'aéroports ou les entreprises qui leur sont liées par contrat. Ces agents doivent être préalablement agréés par le représentant de l'Etat dans le département et le procureur de la République. Ils ne procèdent à la fouille des bagages à main qu'avec le consentement de leur propriétaire et à des palpations de sécurité qu'avec le consentement de la personne. Dans ce cas, la palpation de sécurité doit être faite par une personne du même sexe que la personne qui en fait l'objet ». Cette loi a initié un retrait progressif de l'État dans l'exécution matérielle de la sûreté au profit d'intervenants privés ; celui-ci exerçant néanmoins un rôle d'encadrement de ladite compétence externalisée. Puis, on a assisté à une multiplication de lois en la matière en peu de temps. Mentionnons ainsi la loi du 15 novembre 2001 relative à la sécurité quotidienne, la loi du 18 mars 2003¹²⁶³ et la loi d'orientation et de programmation pour la performance de la sécurité du 12 mars 2011 (LOPPSI) qui viendront confirmer un changement de paradigme dans le milieu aéroportuaire. Désormais, les autorités publiques ne dirigeront plus l'activité privée à travers des « ordres » mais la superviseront à travers un « contrôle »¹²⁶⁴.

Selon Hadrien Protar, les agents privés vont depuis lors s'imposer comme les « principaux exécutants de la sûreté » tandis que les autorités publiques se sont mises à assumer une mission de contrôle de cette activité¹²⁶⁵ en leur donnant une plus grande autonomie. Désormais, les autorités de l'État n'interviennent qu'en dernier recours. À titre d'exemple, lorsqu'un passager refuse de se faire contrôler, les agents privés ont la possibilité de faire appel à un superviseur qui tentera de convaincre le passager récalcitrant. Dans le cas d'un refus catégorique du passager, l'accès lui sera refusé par les agents privés. Et s'il tente de forcer le passage, les agents feront appel aux agents des forces de l'ordre.

¹²⁶³ Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

¹²⁶⁴ H. PROTAR, *La sûreté aéroportuaire en France*, Mémoire de Master, Université Panthéon-Assas-Paris II, 2016.

¹²⁶⁵ Ibidem

De nos jours, l'action d'entités et de personnes privées dans les aéroports prend principalement deux formes : d'une part, une intervention aux côtés des autorités publiques afin de sécuriser certaines zones liées aux migrations ; d'autre part, une assistance des forces publiques dans le cas où des étrangers retenus en situation irrégulière sont amenés à être transportés. Ces deux missions montrent que l'État n'assume plus seul certaines missions en relation avec l'exercice des compétences régaliennes. Dans ce contexte, le partenariat public-privé utilisé pour permettre ces opérations de contrôle par des acteurs privés en vue d'assurer la sécurité aux frontières est de moins en moins contesté ¹²⁶⁶.

Cela étant dit, la délégation du public vers le privé devrait, en théorie, être écartée dans ce domaine puisque les acteurs privés ne se substituent pas aux autorités publiques compétentes mais viennent agir en complément dans le but de décharger ces dernières de certaines missions. Cependant, le bon fonctionnement des plateformes aéroportuaires requiert aujourd'hui la mobilisation de ces personnes et entités privées afin de garantir la sécurité dans ces lieux extrêmement sensibles du point de vue de la sécurité des usagers. Les derniers attentats survenus en Europe, en Belgique notamment, l'ont rappelé. En France, les opérateurs privés se voient appliquer les dispositions déontologiques prévues au Livre VI du Code de la sécurité intérieure. Par ailleurs, le contrôle réalisé par les personnes privées ne doit pas se confondre avec les missions d'inspection ou de filtrage effectuées dans les aéroports. Dans ce cas, le périmètre d'intervention des opérateurs privés concerne seulement la prévention des malveillances dirigées contre le moyen de transport ¹²⁶⁷.

Cette tendance témoigne toutefois des limites de l'action de la puissance publique dans plusieurs secteurs, en particulier celui du contrôle des frontières, qui subissent les aléas de la contrainte budgétaire. Pour autant, l'augmentation des forces publiques de sécurité ne suffirait plus ; les missions de gestion des flux migratoires sont désormais tellement nombreuses et diverses que les seuls moyens des autorités publiques seraient de toute façon insuffisants ¹²⁶⁸.

¹²⁶⁶ X. LATOUR, « La participation des personnes privées au contrôle des migrations en France », *Actualité Juridique Droit Administratif*, Dalloz, 2019, p. 264.

¹²⁶⁷ Ibidem

¹²⁶⁸ X. LATOUR, « La sécurité privée ou l'État autrement », in P. Brajeux, E. Delbecque et M. Mathieu (dir.), *Sécurité privée, enjeu public*, Armand Colin, 2013, p. 215.

§ 2 – La participation aux missions de sécurité contestée des personnes privées dans les aéroports

La participation d'intervenants privés en appui des forces publiques a fait l'objet de critiques. D'ordre politique, une première critique met en cause les mouvements d'externalisation des compétences publiques, notamment lorsqu'il s'agit du traitement des migrants en détresse dont l'État se délaïsse. Les associations de soutien aux migrants dénoncent ainsi une double externalisation : géographique avec le renvoi de la gestion des migrants à des États tiers ou juridique avec une sous-traitance de cette activité à des personnes privées. Ces associations ont souligné les limites d'une telle externalisation, par exemple dans le cas britannique. La Border Force, l'agence responsable des opérations de contrôle frontalier dans les ports aériens, maritimes et ferroviaires du Royaume-Uni qui dépend du Home Office, le ministère en charge des affaires intérieures du pays, a recours à des intervenants privés anglais pour la gestion des frontières, à Calais notamment. Or ceux-ci disposent parfois de marges de manœuvre opérationnelles bien plus importantes que leurs homologues français, ce qui suscite des craintes vis-à-vis du respect des libertés publiques et des droits de l'Homme en général.

Une deuxième critique, d'ordre juridique, conteste la délégation de pouvoirs de police à des personnes privées. Cela a freiné la volonté des États de décharger complètement les forces publiques. Aujourd'hui, les intervenants privés ne peuvent agir que sous l'autorité, et sous la responsabilité, des agents des forces publiques. Cette formule permettrait une certaine « mixité des personnels » dans un environnement juridique plus conciliant¹²⁶⁹. Toutefois, cette mixité est à interpréter comme une coopération, non une action conjointe, car la question de la substitution reste un sujet sensible dès lors que l'action des intervenants, notamment dans l'utilisation de la force, peut être interprétée comme une contrainte illégitime. Cette limite peut être envisagée de manière favorable par les associations de défense des migrants mais ne soulage pas les forces de police de la multitude d'activités dont elles sont investies.

Une troisième et dernière critique met en question la fiabilité des prestataires privés en raison du lien entre les missions exercées et les enjeux de souveraineté. En France, le cadre des missions des intervenants privés est continuellement renforcé, depuis 1983¹²⁷⁰, par le pouvoir législatif et réglementaire, dans un double objectif de professionnalisation et de consolidation. Le Conseil national des activités de sécurité (ci-après CNAPS) est chargé de veiller à la réalisation de ces objectifs. Les autorités françaises pensaient avoir réalisé l'essentiel en

¹²⁶⁹ X. LATOUR, « La participation des personnes privées au contrôle des migrations en France », *Actualité Juridique Droit Administratif*, Dalloz, 2019, p. 264.

¹²⁷⁰ Ibidem

consolidant l'arsenal juridique en matière de sécurité privée, à travers notamment des partenariats. Toutefois, la Cour des comptes a rendu des observations mitigées dans son rapport annuel de 2018 en dénonçant des carences du CNAPS dans la délivrance des agréments, jugée laxiste, et le contrôles des activités dont les défaillances n'ont pas été sanctionnées de manière rigoureuse. Par ailleurs, la Cour des comptes a jugé que les intervenants privés offraient des prestations de qualité irrégulière, réalisées par un personnel aussi mal rémunéré que mal formé. La responsabilité de l'État n'a pas été épargnée puisqu'il serait responsable, selon la juridiction, de la mauvaise réalisation de ces activités en encourageant « indirectement des prestations bas de gamme en donnant la priorité au moins-disant »¹²⁷¹. Ces réserves n'ont toutefois pas remis en cause la participation du privé dans le secteur aéroportuaire dans la mesure où, d'une part, le prestataire privé n'empêche pas l'État d'exercer ses compétences régaliennes, les autorités publiques exerçant des contrôles complémentaires et, d'autre part, il est aujourd'hui admis que l'action de professionnels privés de la sécurité apporte un concours nécessaire aux forces publiques¹²⁷².

Cette collaboration appelle une réflexion sur le continuum de sécurité public-privé dans le transport aéroportuaire où il existe une réelle volonté de décharger les autorités publiques face à l'accroissement de leurs activités. La privatisation de la sécurité se heurte à des défis réels qui empêchent le législateur de formuler une répartition claire des compétences, ce d'autant plus qu'il manque une doctrine française solide sur la question de l'emploi de la sécurité privée dans le milieu aéroportuaire. L'extrême sensibilité qui entoure un sujet au cœur des enjeux de souveraineté et des compétences régaliennes ne rend pas le débat plus apaisé. L'État, dans son rôle de régulateur, sera amené dans le futur à donner des gages vis-à-vis de la fiabilité et de l'utilité des partenariats public-privés.

Sous-section 2 – Les défis du traitement des données aux frontières au regard de l'ingérence des acteurs privés

En accueillant des millions de voyageurs par an¹²⁷³, les aéroports doivent assurer à la fois un bon fonctionnement et un haut niveau de sécurité. La sécurité aéroportuaire, gérée par des acteurs privés, requiert ainsi de traiter une masse importante de données personnelles des passagers aériens. Avec diverses méthodes, les transporteurs et des experts en sécurité, interviennent de plus en plus aux côtés des autorités publiques dans la gestion des

¹²⁷¹ Ibid.

¹²⁷² Ibid.

¹²⁷³ J. PAVAUX, « Quel est le vrai bilan socio-économique des aéroports français ? », *Jacques Pavaux Conseil*, 30 novembre 2021.

frontières¹²⁷⁴. Arrivé devant les frontières, le voyageur voit ses données collectées et traitées par ces divers acteurs. L'efficacité de cette collecte et la protection effective des droits des passagers aériens se posent comme des défis juridiques majeurs, notamment du point de vue de la garantie des droits fondamentaux, en particulier la protection de la vie privée et des données à caractère personnel.

§1 - Les acteurs privés au défi des actions en justice formées contre les transporteurs aériens

L'industrie du transport aérien est actuellement confrontée à de nombreux changements qui participent à un réexamen des modèles économiques existants en produisant des effets considérables sur les territoires et les passagers. Ces mutations sont de différentes sortes. Depuis la libéralisation de l'espace aérien européen en 1997¹²⁷⁵, le double phénomène de l'émergence des compagnies low-cost et de la montée en puissance des compagnies aériennes du Golfe et turques, la concurrence entre compagnies aériennes s'est intensifiée. En outre, différents défis se posent en termes de disponibilité et d'opportunité des ressources publiques pour développer les plateformes aéroportuaires en ayant un retour sur investissement. Par ailleurs, du point de vue du droit européen, les nouvelles lignes directrices sur les aides d'État sont mal comprises par les propriétaires et les gestionnaires de plateformes aéroportuaires qui les voient comme intrusives.

De plus, même si le développement du trafic aérien s'accompagne d'une efficacité énergétique toujours croissante, ce mode de transport contribue au changement climatique. Dans un environnement hautement concurrentiel, l'industrie aéronautique en Europe bénéficie d'un régime plutôt favorable pour taxer ses externalités environnementales, les taxes sur les carburants étant exonérées tant au niveau international qu'à l'échelon national, notamment de la taxe intérieure sur la consommation de produits énergétiques (TICPE). D'un point de vue international, la détaxation du kérosène pour les vols internationaux est conforme aux recommandations de l'OACI et aux exigences de l'article 24 de la Convention de Chicago relative à l'aviation civile internationale. Néanmoins, l'industrie du transport aérien international, qui croît à un rythme annuel moyen de 5 %, s'efforce d'améliorer son efficacité énergétique.

¹²⁷⁴ M. BERGADAÀ, « Le temps économique et le temps psychologique du voyageur dans un aéroport international », *La revue des sciences gestion*, 2009/2, n° 236, pp. 12-23.

¹²⁷⁵ Gouvernement, « Rapport sur le maillage aéroportuaire français », *Conseil supérieur de l'aviation civile*, 2017.

Cette mutation du droit aérien touche également les droits de trafic¹²⁷⁶ qui sont totalement libéralisés dans le cadre des accords conclus entre l'Europe et les États-Unis et le Canada en échange de la convergence de l'ensemble des réglementations applicables au transport aérien. Dans un cadre bilatéral, chaque pays impose sa propre réglementation et régule l'accès au marché aérien en fixant mutuellement des enveloppes de capacité pour les compagnies aériennes des deux pavillons, celles-ci étant régulièrement ajustées en fonction de l'évolution de la demande. Si dans les accords bilatéraux entre la France et le Brésil, le Japon, l'Inde, l'Afrique du Sud, ou encore la Turquie, le périmètre des enveloppes de capacités de production laisse une large marge de développement aux entreprises, ces enveloppes sont plus restreintes avec des pays comme la Russie, la Chine, les Émirats Arabes Unis et le Qatar. Pour ces deux derniers États, la Commission européenne a reçu, en 2016, un mandat des États membres en vue de négocier un accord cadre inspiré des accords avec les États-Unis et le Canada.

Au sein de l'Union européenne, des règles communes ont pour but de garantir un niveau minimum d'assistance aux passagers de tous les modes de transport en cas de retards prolongés ou d'annulations mais également à protéger en particulier les voyageurs les plus vulnérables. Cependant, les dérogations possibles au transport ferroviaire ou routier sont nombreuses et les litiges devant les tribunaux sont encore fréquents. La législation européenne sur les droits des passagers vise ainsi à fournir une protection minimale et uniforme aux passagers de tous les modes de transport afin de faciliter les déplacements et d'encourager l'utilisation des transports collectifs¹²⁷⁷.

Cet arsenal juridique spécifique aux transports s'ajoute à celui relatif à la protection des consommateurs et aux voyages à forfait, aux accords internationaux applicables, à la Charte des droits fondamentaux et aux règles nationales pertinentes. Cet ensemble de règles établit des droits de « base » communs à tous les modes de transport : protection particulière des passagers à mobilité réduite, non-discrimination, information des voyageurs, organismes nationaux de contrôle et systèmes de traitement des plaintes. Des mécanismes d'assistance et de compensation pour les vols annulés ou fortement retardés pour chaque mode de transport ont notamment été mis en place¹²⁷⁸.

¹²⁷⁶ Ibidem

¹²⁷⁷ Parlement européen, « Les droits des passagers », *Les fiches thématiques de l'Union européenne*, avril 2023, en ligne à URL : <https://www.europarl.europa.eu/factsheets/fr/sheet/48/les-droits-des-passagers> consulté le 27 juin 2023.

¹²⁷⁸ Ibidem

En plus des incidents d'exploitation, comme les retards de vols, pour lesquels leur responsabilité peut être mise en cause, les transporteurs aériens font aujourd'hui face à d'autres risques, notamment ceux liés au développement des nouvelles technologies¹²⁷⁹. En principe, l'action en justice en droit français est personnelle puisqu'elle est rattachée à la personne même de l'individu qui l'initie. Toutefois, le législateur a ouvert le droit aux actions collectives formées par ou au nom d'un groupe de personnes à travers la loi du 17 mars 2014, dite « loi Hamon », qui a introduit l'action de groupe dite « consommation ». Cette action, qui n'a pas engendré une augmentation des contentieux comme les transporteurs redoutaient¹²⁸⁰, n'est pas exempte d'intérêt pour les acteurs du transport aérien. Ces derniers ont par ailleurs vu l'apparition d'un nouveau type d'action de groupe portant sur les données personnelles.

En effet, cette action de groupe a été étendue, par la loi dite « J21 » du 18 novembre 2016 à d'autres domaines que ceux prévus jusqu'alors en matière de consommation¹²⁸¹. Dans ce cadre, le législateur a intégré l'action de groupe dite « données personnelles » initialement prévue pour faire cesser un manquement aux droits consacrés par la Loi Informatique et Libertés du 6 janvier 1978¹²⁸² (LIL) tels que le droit à l'information, d'opposition, d'accès ou de rectification. Mais le domaine de cette action couvre aujourd'hui d'autres droits. Dans le contexte du RGPD, la loi du 20 juin 2018¹²⁸³, dans son article 16, a étendu l'action de groupe à la réparation des préjudices matériels et moraux. Ainsi, cette action permet aujourd'hui à un groupe de former une action judiciaire pour obtenir la cessation d'un manquement et la réparation des préjudices subis. Pour que l'action aboutisse à un résultat satisfaisant, les personnes physiques identifiées ou identifiables doivent être placées dans une situation similaire et subir un dommage ayant pour cause commune un manquement de même nature commis par un même professionnel. Les passagers aériens peuvent ainsi se retourner vers les transporteurs aériens en leur qualité de responsables de traitement¹²⁸⁴ lorsque ces derniers n'ont pu éviter une violation de leurs données.

Cette action peut viser, à la fois, les cyberattaques et les manquements plus généralement imputables aux responsables de traitement et relatifs à la réglementation sur les données personnelles. Le groupe en question ne devrait pas rencontrer beaucoup de difficultés pour

¹²⁷⁹ S. PARIER, « L'action de groupe et le RGPD en matière de transport aérien », *Juris tourisme*, Dalloz, n° 215, 2019, p. 44.

¹²⁸⁰ Ibidem

¹²⁸¹ L. n° 2016-1547 du 18 nov. 2016, JO du 19 nov. 2016.

¹²⁸² Cette loi, relative à l'informatique, aux fichiers et aux libertés, régit le traitement des données personnelles en France.

¹²⁸³ L. n° 2018-493 du 20 juin 2018, JO du 21 juin 2018.

¹²⁸⁴ Une personne définissant les finalités et les moyens d'un traitement de données personnelles.

former leur action, car toute violation de données doit, en principe, faire l'objet d'une déclaration auprès des services de la CNIL et, le cas échéant, des personnes concernées par la collecte. Les justiciables peuvent ainsi compter sur les avantages fédérateurs de la mutualisation des coûts qu'offre ce type d'action en justice. Toutefois, bien qu'elle soit facilitée, l'action de groupe doit respecter un cadre procédural strict pour que la mise en cause du transporteur aérien, en sa qualité de responsable de traitement, puisse aboutir.

Le transporteur aérien, à l'instar de tout autre responsable traitement, devra avoir été, au préalable à son introduction, mis en demeure pour faire cesser ou réparer un préjudice. Ce n'est qu'à l'expiration d'un délai de quatre mois, à compter de la réception de cette mise en demeure, qu'une action de groupe pourra être intentée devant la juridiction compétente¹²⁸⁵. Une fois saisi, le tribunal statuera sur les conditions d'engagement de la responsabilité du professionnel visé par l'action et fixera, ensuite, le délai dans lequel les personnes concernées pourront demander leur adhésion au « groupe ». Le jugement pourra faire l'objet de mesures de publicité afin d'assurer l'information des personnes susceptibles d'adhérer au groupe. La dernière étape sera, enfin, la mise à exécution du jugement. Sous réserve du respect de ce cadre procédural, l'action de groupe relative aux données personnelles pourra ainsi permettre aux voyageurs victimes d'une violation de leurs données personnelles d'obtenir la cessation de toutes atteintes ou la réparation du préjudice qu'ils auraient pu subir du fait de violations relevées à l'encontre du transporteur aérien concerné.

§ 2 - La multiplication des menaces contre les installations aéroportuaires pour les acteurs privés

La nécessité d'assurer le maintien d'un niveau élevé de sûreté dans les aéroports est aujourd'hui un défi crucial pour les acteurs de ce secteur compte tenu de la multiplication des menaces, sous diverses formes, contre les installations aéroportuaires. Si l'histoire du transport aérien est jalonnée d'actes de malveillance qui ont débouché parfois sur des drames de masse, ce secteur se heurte de nos jours à une limite majeure : celle de l'adaptation. D'après l'article L. 6341-2 du Code des transports, l'exploitant de l'aéroport est le premier responsable de la mise en œuvre de la politique de sûreté sur la plateforme aéroportuaire. S'il peut à cet égard recourir aux services d'acteurs professionnels pour externaliser cette tâche, il lui appartient en principe de s'assurer que toutes les mesures nécessaires sont prises suivant les conditions précisées dans un contrat contraignant signé avec l'État visant à empêcher toute atteinte illicite

¹²⁸⁵ L. n° 2016-1547, préc., art. 64.

à la plateforme aéroportuaire. En règle générale, les deux parties signent un contrat de concession de service public¹²⁸⁶.

Face à de nouveaux dangers, notamment les vols illégaux de drones autour des aéroports, les cyberattaques contre les aéroports et les risques accrus de terrorisme contre ces plateformes, les exploitants sont mis devant les défis d'une réaction rapide et l'adoption de nouvelles mesures de sûreté. En raison du développement de la technologie et de l'obsolescence rapide des équipements de détection, la mise en place de dispositifs renforçant la sûreté est donc de plus en plus urgente.

Ainsi, les acteurs du secteur vont assister à une sérieuse augmentation des coûts liés aux mesures que prendront les opérateurs. Outre le débat sur les mesures à prendre pour prévenir ces nouveaux risques variables, les autorités doivent également répondre à la difficile question de savoir sur qui devra peser les coûts : les opérateurs, les passagers, les compagnies aériennes ou d'autres acteurs ?

Pour les acteurs privés, les nouvelles menaces pesant sur les plateformes aéroportuaires comprennent les cyberattaques et le risque de radicalisation touchant les travailleurs des aéroports. Les données des passagers aériens peuvent être touchées par ces phénomènes.

Au fil des années, les aéroports sont devenus des interfaces par lesquelles transitent les personnes, les marchandises et surtout les données, à tel point qu'il est d'usage de parler aujourd'hui d'aéroports « connectés ». Ces plateformes sont désormais des lieux privilégiés pour collecter et traiter des milliers de données. L'augmentation du volume de données traitées est intrinsèquement liée au développement des services offerts aux passagers par les aéroports. Pour s'en assurer, il suffit de se référer à l'article R. 232-6 du code de la sécurité intérieure et au dispositif dit « Parafe »¹²⁸⁷ qui permet d'accélérer le franchissement des frontières pour les voyageurs, notamment ceux en provenance de l'Union européenne qui disposent d'un passeport biométrique, en contrepartie d'une inscription dans un registre dédié et donc en contrepartie de la collecte de données personnelles¹²⁸⁸.

Dans le cas des données des dossiers passagers comme celles des compagnies aériennes (communication des données de vol au gestionnaire), les données collectées par les aéroports,

¹²⁸⁶ S. PARIER, « Entre prévention de nouvelles menaces et défis à relever pour l'exploitant », *Tourisme & territoire, Sûreté aéroportuaire, Juris Tourisme*, Dalloz, n° 208, 2018, p. 38.

¹²⁸⁷ A. GALY, « La gestion des frontières par le traitement différencié des voyageurs. Réflexion croisée sur la France et les États-Unis », *Critique internationale*, vol. 93, n° 4, 2021, pp. 137-155.

¹²⁸⁸ S. PARIER, « Entre prévention de nouvelles menaces et défis à relever pour l'exploitant », *Tourisme & territoire, Sûreté aéroportuaire, Juris Tourisme*, Dalloz, n° 208, 2018, p. 38.

et surtout leur protection apparaissent comme une question centrale dans la détermination de la politique de sûreté de l'exploitant. La nécessité de protéger « la confidentialité, l'intégrité et la disponibilité des systèmes et données informatiques et de communications critiques utilisées aux fins de l'aviation civile contre des interventions qui peuvent compromettre la sécurité de l'aviation civile »¹²⁸⁹ est ainsi consacrée pour permettre l'atteinte de cet objectif de protection des droits fondamentaux des passagers aériens.

La sûreté désigne l'ensemble des moyens mis en œuvre pour la prévention des actes de malveillance¹²⁹⁰. Ces dix dernières années, plusieurs aéroports ont été amenés à tester leur capacité de répondre à de tels actes malveillants : des cyberattaques ou d'autres types d'attaques sur les aéroports ont visé celui d'Istanbul en 2013, celui de Londres en 2014, celui de Varsovie en 2015, celui de Bruxelles en 2016, ou encore celui de Kiev en 2017. Les exploitants sont ainsi appelés à réagir pour protéger leur système d'information et de traitement des données contre des tiers malveillants¹²⁹¹. En France, les exploitants sont tenus, en vertu de l'application du règlement n° 2016/679 du 27 avril 2016 relative à la protection des données personnelles et du fait de leur statut d'opérateur d'importance vitale (OIV), de prendre ce type de mesures. En effet, les aéroports sont astreints à des obligations particulières dans la mesure où ils sont perçus comme des lieux sujets à une atteinte à la sécurité de la Nation et une diminution du potentiel économique, voire de la capacité de guerre du pays.

Dans ce contexte, nous devons noter l'entrée en vigueur de la directive SRI 2¹²⁹² qui vise à renforcer la protection des systèmes d'information au sein de l'Union européenne à l'encontre d'acteurs malveillants de plus en plus cyniques et performants. Cette directive considère les transports comme un secteur essentiel au sein de l'Union européenne, caractérisé par un réseau de services de plus en plus interdépendants et transfrontaliers¹²⁹³. Les États membres sont donc appelés à utiliser les technologies innovantes, y compris l'intelligence artificielle, pour détecter et prévenir les cyberattaques contre ces secteurs essentiels de leur économie. Les aéroports sont cités dans l'annexe de la directive comme « secteur hautement

¹²⁸⁹ Ibidem

¹²⁹⁰ R. CARTER, « Chapitre premier. Les transports aériens : un risque identifié, une menace globalisée », *La sûreté des transports. Les transports face aux risques et menaces terroristes*, sous la direction de Carter Raymond H. A. Presses Universitaires de France, 2008, pp. 13-109.

¹²⁹¹ J. NOCETTI, « Géopolitique de la cyber-conflictualité », *Politique étrangère*, n° 2, 2018, pp. 15-27.

¹²⁹² Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

¹²⁹³ Directive SRI 2, considérant 37.

critique »¹²⁹⁴. Récemment, une panne informatique mondiale a paralysé des entreprises du monde entier et des secteurs essentiels comme les aéroports¹²⁹⁵. Elle confirme la persistance des menaces informatiques sur les aéroports. La directive encourage la mise en place de mesures techniques, opérationnelles et organisationnelles nécessaires pour garantir la sécurité de ces secteurs.

Cette menace n'a pas été minimisée les autorités compétentes, c'est pourquoi les opérateurs ont pris les mesures nécessaires afin de garantir l'intégrité de leurs systèmes d'information mais surtout se prémunir contre les conséquences d'une éventuelle cyberattaque en souscrivant une assurance pour se protéger contre ce risque sachant qu'il est aujourd'hui accru. Par exemple, discrets et pratiques, des drones peuvent aussi être utilisés comme des « relais et vecteurs d'actes cybercriminels »¹²⁹⁶. Précisément, l'exploitant est responsable d'assurer la protection de l'infrastructure et la sécurité des personnes travaillant dans l'aéroport. Dans le cadre de ses fonctions de sûreté, il doit mettre en place un certain nombre de mesures visant à réduire les risques d'ingérence malveillante sur le site aéroportuaire. L'une des principales mesures dans ce domaine est le zonage¹²⁹⁷ qui consiste pour les gestionnaires à définir les parties de l'aéroport librement accessibles au public de celles qui ne le sont pas. Concrètement, les autorités compétentes procèdent à une délimitation pour garantir l'inviolabilité des zones dont l'accès est restreint. Cela passe par la mise en place d'obstacles matériels comme l'installation de points de contrôle d'accès ou encore la pose de barrières.

Construire un véritable réseau de plateformes aéroportuaires est indispensable pour la consolidation des mesures de sûreté et s'inscrit dans une volonté de protéger ces zones en interdisant l'accès à tout élément pouvant compromettre la sécurité de l'avion et de ses passagers. Pour autant, ces dispositifs semblent aujourd'hui insuffisants pour prévenir une nouvelle menace venue du ciel : le survol de drones civils. Alors que les cas de drones survolant des lieux sensibles, notamment les aéroports et leurs abords, se sont multipliés ces dernières années, les opérateurs ne peuvent ignorer le risque que ce nouveau type de péril aérien fait peser sur la sécurité de leurs plateformes.

Dès 2016, le Bureau d'enquêtes et d'analyses (BEA) indiquait qu'il y avait eu plusieurs collisions entre des drones et des avions de ligne alors qu'ils s'apprêtaient à atterrir à l'aéroport

¹²⁹⁴ Directive SRI 2, annexe.

¹²⁹⁵ France info, « Panne informatique mondiale : ce que l'on sait du bug entre Microsoft et CrowdStrike, qui a paralysé des entreprises du monde entier », *France Télévisions*, 19 juillet 2024.

¹²⁹⁶ S. PARIER, « Entre prévention de nouvelles menaces et défis à relever pour l'exploitant », *Tourisme & territoire, Sûreté aéroportuaire, Juris Tourisme*, Dalloz, n° 208, 2018, p.38.

¹²⁹⁷ Ibidem

Charles de Gaulle. Les exemples de drones survolant les aéroports se sont multipliés bien que cela soit interdit par la loi. En effet, l'article L. 6211-4 du Code des transports précise que « le survol de certaines zones du territoire français peut être interdit pour des raisons d'ordre militaire ou de sécurité publique dans des conditions fixées par décret en Conseil d'État »¹²⁹⁸. Ainsi, tout pilote à distance qui enfreint cette règle et opère à proximité d'un aéroport risque une condamnation pénale.

Bien que les professionnels du secteur appellent à relativiser le risque de collision, l'utilisation malveillante probable des drones, notamment à des fins terroristes, tend à limiter cette allégation. Les opérateurs, qu'ils soient amateurs désarmés ou purement malveillants, auront la plus grande difficulté à faire respecter l'interdiction de survol existante, en dehors bien entendu de l'obtention des moyens de détection et d'interception nécessaires. Au vu des expérimentations réalisées, dont le dispositif « Hologarde »¹²⁹⁹ testé à l'aéroport Charles de Gaulle, c'est encore une position que semblent prendre certains responsables. En effet, les aéroports de Francfort, de Dubaï, de Dublin, de Newark, de Heathrow, pour ne citer que quelques aéroports, ont vu leur activité perturbée par des vols illicites de drones. Alors que cette menace était inexistante il y a quelques années, en 2019, les spécialistes ont compté près de 2000 incidents par an impliquant ce type d'incidents, aux bords de sites critiques. Le même nombre d'incident a été enregistré aux États-Unis¹³⁰⁰.

Cette situation entraîne plusieurs conséquences pour les aéroports dont l'annulation de certains vols et le déroutement d'autres, voire l'interruption du fonctionnement de l'aéroport, comme celui de Gatwick, aux alentours de Londres, qui a dû être fermé pour trois jours en décembre 2019, bloquant ainsi 140 000 passagers et 1000 vols¹³⁰¹. L'attaque de drone a coûté 1,4 million de livres sterling à l'aéroport. Alors que les premières estimations des coûts s'élevaient à des dizaines de millions de livres sterling, le poids a été supporté par les compagnies aériennes. L'aéroport de Gatwick a depuis dépensé 4 millions de livres sterling supplémentaires pour se doter d'une technologie anti-drone¹³⁰².

La sûreté de l'aéroport préoccupe également aujourd'hui les gestionnaires qui sont confrontés à une autre menace contemporaine : la radicalisation des travailleurs du secteur aéroportuaire.

¹²⁹⁸ Code des transports, article L. 6211-4.

¹²⁹⁹ O. JAMES, « L'aéroport de Roissy déploie un arsenal antidrones », *Hologarde*, 8 juin 2019, en ligne à URL : <https://hologarde.com/wp-content/uploads/2019/06/UsineNouvelle-Hologarde.pdf> consulté le 25 juin 2023

¹³⁰⁰ Ibidem

¹³⁰¹ G. TOPHAM, "Gatwick drone disruption cost airport just £1.4m", *Guardian*, 18 juin 2019, en ligne à URL : <https://www.theguardian.com/uk-news/2019/jun/18/gatwick-drone-disruption-cost-airport-just-14m> consulté le 25 juin 2023.

¹³⁰² Ibidem

En effet, l'aéroport est divisé en divers zones. Le maillage de la plateforme est l'une des bases de la politique de sûreté des exploitants. Les zones divisées sont classées en fonction de leur degré de criticité : zone côté, piste, à accès réglementé, etc. Cette classification vise à restreindre l'accès de certaines parties de la plateforme aéroportuaire à une catégorie de personnes autorisées¹³⁰³.

Les passagers sont les premiers concernés par le zonage comme le montre l'exemple de la mise en place de point d'accès filtrage (PIF) qui a pour finalité de ne donner l'accès à la salle d'embarquement qu'aux passagers ayant une carte pour embarquer. Cela permet de maintenir les individus qui en sont dépourvus dans la partie publique librement accessible de l'aéroport. Le plus souvent, ce sont les personnes du secteur privé, évoluant sur la plateforme, qui sont concernées par cette mesure de sûreté. L'opération de zonage de l'aéroport entraîne des conséquences sur le personnel non-détenteur de la carte d'accès puisque la mesure de sûreté impose à ces individus des contrôles, fréquents mais nécessaires, de leur accès sur la plateforme. Le but est d'éviter l'intrusion d'individus mal intentionnés dans ces zones sensibles en termes de sûreté aérienne.

Afin de pouvoir circuler au sein de ces espaces, tout membre du personnel présent sur la plateforme doit présenter une pièce d'identité valide et à jour¹³⁰⁴. Délivrée dans le cadre d'une habilitation départementale, cette carte d'identité est une garantie d'intégrité exemplaire et morale pour le porteur. Elle prouve notamment que ce dernier n'a commis aucun acte incompatible avec la conduite des activités dans les zones de l'aéroport qui ne sont pas librement accessibles. En cas de non-respect de cette condition, l'autorité administrative a le droit de refuser d'accorder une telle autorisation. Il est à noter que la licence peut également être suspendue ou révoquée si le titulaire ne remplit plus les conditions ci-dessus énoncées. Corrélativement, il peut y avoir une suspension ou révocation de la carte d'identité du personnel fautif, lui permettant de circuler sur la plateforme.

Du point de vue de la jurisprudence, les juges du tribunal de première instance semblent avoir pris position en faveur de la prévention de tout comportement dangereux pour garantir la sécurité publique, en l'espèce la sécurité aéroportuaire. Ainsi, le fait d'entretenir des relations avec des radicaux intégristes qui ont évolués dans la « mouvance salafiste »¹³⁰⁵ est incompatible avec le fait d'opérer dans la zone réservée de l'aéroport, ce qui justifie la

¹³⁰³ S. PARIER, « Entre prévention de nouvelles menaces et défis à relever pour l'exploitant », *Tourisme & territoire, Sûreté aéroportuaire*, *Juris Tourisme*, Dalloz, n° 208, 2018, p. 38.

¹³⁰⁴ Ibidem

¹³⁰⁵ CAA Versailles, 12 octobre 2009, req. n° 08VE02693.

révocation immédiate de l'autorisation départementale. S'il existe une variété de motivations pour révoquer les permis départementaux, le contexte actuel de lutte contre les mouvements djihadistes et le risque élevé d'attentats terroristes tendent à alimenter le débat autour de la radicalisation des travailleurs des aéroports et de leurs sous-traitants.

De plus, l'émergence de nouvelles menaces oblige les exploitants d'aéroports à prendre les mesures nécessaires pour les prévenir d'où une augmentation des dépenses de sûreté aéroportuaire depuis 2001¹³⁰⁶. Les recherches dans ce domaine montrent que le coût total des mesures de sûreté mises en place par les exploitants aéroportuaires français en 2016 était déjà d'environ 766 millions d'euros¹³⁰⁷. Le développement de réglementations, toujours plus strictes, en matière de sûreté pour se prémunir contre les nouveaux risques susmentionnés laisse penser que la facture sera encore plus élevée à l'avenir.

Se pose alors la question du financement de la sûreté sur la plateforme aéroportuaire¹³⁰⁸. Si ce coût est actuellement financé par les taxes d'aéroport, que toutes les compagnies aériennes de passagers paient et ajoutent au prix du billet payé par les passagers, il est prévisible que ces prélèvements ne suffiront plus dans un avenir proche. Les principaux acteurs doivent donc envisager de nouvelles mesures en prenant en compte les coûts qui varient. Si des augmentations de prix sont envisageables, d'autres solutions sont à l'étude, puisque les taxes d'aéroport ont déjà un impact significatif sur la compétitivité des aéroports français considérés comme onéreux par rapport à leurs homologues européens.

Par ailleurs, une augmentation du montant de la taxe tend à pénaliser les compagnies aériennes qui ne pourront plus répercuter l'intégralité de la taxe sur les billets vendus. Cette situation sera donc néfaste économiquement pour les aéroports français qui, de fait, risquent de souffrir de la prise de distance des passagers pour les compagnies aériennes française. Certains privilégieraient d'étendre l'assiette de la taxe aux vols privés, puisque ces derniers fonctionnent de la même manière que les vols commerciaux de passagers et bénéficient des mêmes mesures de sûreté prises par l'opérateur. De ce fait, la question des garanties et de leur financement est loin d'être résolue. La mise en place de nouvelles mesures de sûreté pour prévenir la menace d'exposition, et ainsi maintenir un haut niveau de protection des infrastructures aéroportuaires, n'est pas sans conséquences pour les données personnelles des

¹³⁰⁶ M. BOUCTON et S. PARIER, « La sûreté aéroportuaire : oui, mais à quel prix ? », *Air & Cosmos*, octobre 2017, n° 2564.

¹³⁰⁷ Ibidem

¹³⁰⁸ R. CARTER, *La sûreté des transports. Les transports face aux risques et menaces terroristes*. Presses Universitaires de France, 2008.

passagers aériens qui sont, conséquemment, amenées à être traitées et utilisées par d'autres acteurs¹³⁰⁹.

Section 2 – La mise en danger de la protection juridique des dossiers passagers par la privatisation des aéroports

Au cours des dernières années, certaines innovations ont été constatées dans le secteur aéroportuaire (sous-section 1). L'accent est mis sur la transformation numérique, l'automatisation et l'efficacité de manière concomitante à la recherche constante, par les aéroports, d'une amélioration de la sûreté et de la sécurité. En France, les évolutions du cadre de la gestion des aéroports ont été marquées par des opérations de privatisation qui ont été justifiées, du point de vue de la puissance publique, par la volonté de s'adapter à la forte concurrence européenne et mondiale ainsi que de réduire la dette publique¹³¹⁰. Dictée par la conjoncture économique internationale, les opérations de privatisation des aéroports (sous-section 2) ont obligé les gouvernements à aménager les régimes applicables des sociétés françaises tout en essayant de protéger l'intérêt général des plateformes aéroportuaires qui jouent un rôle essentiel dans la vie économique, politique et surtout sécuritaire de l'État.

Sous-section 1 – La transformation contemporaine des aéroports par les nouvelles technologies

Une décennie après la crise économique et financière mondiale de 2007-2008, les politiques économiques structurelles et à court terme des pays sont toujours dominées par la modération des dépenses et la rationalisation des investissements publics. Pour certains gouvernements, cette restriction implique la privatisation des actifs de l'État. L'industrie aéroportuaire n'a pas été épargnée par cette tendance. En effet, la privatisation des services publics peut catalyser une intégration technologique accrue, en stimulant l'innovation et en favorisant l'adoption rapide de solutions numériques modernes. C'est pourquoi, les aéroports tendent de plus en plus vers une meilleure intégration technologique ; une tendance qui s'illustre notamment par l'implémentation de l'internet des objets dans les aérogares qui permet de gérer intelligemment et efficacement la maintenance de ces plateformes stratégiques.

¹³⁰⁹ F. JOZEK, « Les ressources extra-aéronautiques des aéroports commerciaux », *Droit et Ville*, vol. 82, n° 2, 2016, pp. 3-18.

¹³¹⁰ R-P. ANDLAUER, « Nouvelle série de privatisations concernant Aéroport de Paris, Française des Jeux et Engie », *CVS Avocats*, Droit des sociétés, 5 septembre 2018, en ligne à URL : https://www.cvs-avocats.com/uploads/media/media/5e68ca2d5128f_option-droit-affaires-nouvelle-se-rie-de-privatisations-concernant-ae-roport-de-paris-francaise-des-jeux-et-engie-rene-pierre-andlauer.pdf consulté le 29 juin 2023.

§ 1 – Les aéroports face à l'intégration du numérique

Dans sa vision pour l'avenir du transport aérien¹³¹¹, l'Association du transport aérien international (International Air Transport Association) aspire à des vols aériens « simples, agréables et sans tracas »¹³¹². Utilisant des composants intégrés de l'internet des objets (*Internet of Things*, IoT) pour apporter des services à valeur ajoutée¹³¹³, les aéroports intelligents (*smart airports*) sont un concept clé de cette nouvelle dynamique qui touche le transport aérien. L'IATA les définit comme des aéroports utilisant « un réseau avec une capacité de réponse pilotée par les données qui d'une part, offre aux voyageurs une meilleure expérience de voyager et d'autre part, vise à garantir un niveau de sécurité plus élevé pour les passagers, opérateurs et le public »¹³¹⁴.

Cette innovation dans le milieu aéroportuaire n'aurait pas été possible sans l'apport de l'internet des objets. Cette technologie se présente comme la troisième révolution de l'internet, le « web 3.0 », grâce à laquelle des milliards de capteurs intégrés dans différents objets du quotidien sont incorporés dans une infrastructure pour enregistrer, traiter et transférer des données¹³¹⁵. Ces objets vont par la suite interagir avec d'autres appareils, dont des objets connectés, mais aussi avec des individus et d'autres systèmes informatiques. Au sein de ce « réseau des réseaux », les objets « connectés » s'identifient et communiquent entre eux à l'aide de systèmes d'identification électronique unifiés et de dispositifs mobiles sans fil. Un ordinateur pilote une application intelligente alimentée par un système de transmission des données. L'internet des objets peut alors être vu comme une série de systèmes indépendants fonctionnant avec leurs propres infrastructures¹³¹⁶. Cela explique pourquoi les chercheurs voient dans ce système non pas un internet étendu au monde physique mais plutôt des applications et des systèmes intégrés à des objets qui utilisent les technologies de l'internet¹³¹⁷.

En intégrant des composants intelligents, les aéroports sont exposés à une surface et des mécanismes de potentielles attaques plus importants. Or, les aéroports doivent garantir chaque jour des niveaux plus élevés de cybersécurité en raison de l'impact potentiel des

¹³¹¹ IATA, Annual Review 2015.

¹³¹² Ibidem

¹³¹³ Transportation Research Board Airport, *A primer to prepare for the connected airport and the internet of things*, Report 19, Cooperative Research Program (ACRP), 2019.

¹³¹⁴ European Union Agency for Network and Information Security, *Securing Smart Airport*, 2016.

¹³¹⁵ D. EMMANUEL, P. FLORA, « Cybersécurité et objets connectés », *Dalloz IP/IT*, 2016, p. 409.

¹³¹⁶ Ibidem

¹³¹⁷ Ibid.

cyberattaques et des perturbations sur la sécurité des passagers et des opérateurs¹³¹⁸. La sensibilisation aux risques de cybersécurité et l'amélioration de la sécurité ainsi que de la résilience de l'ensemble du cycle de vie des opérations aéroportuaires constituent désormais une priorité pour protéger les données personnelles des passagers aériens.

L'interconnexion de toutes ces bases de données à travers des dispositifs est censée offrir un parcours de voyage plus fluide et simplifié aux voyageurs tout en garantissant leur sécurité et celle de leurs biens. La Convention de Chicago rappelle à cet effet l'impératif de protection de « la confidentialité, l'intégralité et la disponibilité des systèmes et données informatiques et de communications critiques utilisées aux fins de l'aviation civile ». Tout transporteur est alors appelé à prendre les mesures nécessaires pour protéger les droits et libertés des passagers aériens faisant l'objet d'une collecte de données. En effet, les transporteurs aériens ne sont pas à l'abri d'attaques susceptibles d'entraîner une fuite des informations personnelles des voyageurs¹³¹⁹.

L'intérêt de l'Union européenne pour le droit des passagers aériens, en particulier pour les données personnelles des passagers, n'est plus une abstraction depuis que le Conseil a adopté la directive le 21 avril 2016 relative aux données des dossiers passagers (PNR)¹³²⁰. Cet ensemble de lois est indispensable pour les autorités européennes, car les activités de la criminalité organisée et du terrorisme impliquent fréquemment des déplacements transfrontaliers. En effet, l'échange de ces données entre autorités répressives a participé de la suppression des contrôles aux frontières intérieures découlant de la Convention de Schengen. L'utilisation des données des passagers aériens n'est qu'un outil parmi d'autres de lutte contre la criminalité transfrontière¹³²¹.

L'utilisation des données personnelles des passagers s'inscrit dans la stratégie européenne de lutte contre le terrorisme¹³²². Adoptée en 2005 par le Conseil, celle-ci vise à « combattre le terrorisme à l'échelle mondiale et rendre l'Europe plus sûre ». Cette stratégie européenne repose sur quatre piliers : la prévention, la protection, la poursuite et la réaction. Comme deuxième priorité, la protection comprend la protection des frontières extérieures, la

¹³¹⁸ S. PARIER, « L'action de groupe et le RGPD en matière de transport aérien », *Juris tourisme*, Dalloz, 2019, n° 215, p. 44.

¹³¹⁹ A. COUNIS, « British Airways victime d'un vaste piratage informatique », *Les Echos*, 6 sept 2018.

¹³²⁰ Conseil de l'Union européenne, « Prévention du terrorisme et de l'extrémisme violent et lutte contre ces phénomènes : le Conseil adopte des conclusions sur l'action extérieure de l'UE », *Communiqué de presse*, 16 juin 2020, <https://www.consilium.europa.eu/fr/press/press-releases/2020/06/16/preventing-and-counteracting-terrorism-and-violent-extremism-council-adopts-conclusions-on-eu-external-action/>.

¹³²¹ Ibidem

¹³²² Conseil de l'Union européenne, « La stratégie européenne de lutte contre le terrorisme », 2005, <https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/eu-strategy/>.

protection des cibles stratégiques, le renforcement de la sécurité dans les transports et la réduction de la vulnérabilité des infrastructures critiques¹³²³. La volonté de protéger les citoyens et les infrastructures ainsi que de réduire leur vulnérabilité aux attentats a poussé l'UE à adopter, en avril 2016, la directive PNR. Pour certains chercheurs, la politique européenne des dossiers passagers fait partie des questions « non-négligeables » au sein de l'espace de l'Union européenne de ces dernières années bien que les débats politiques ne les aient pas toujours mises en avant¹³²⁴.

Du PNR à la réforme du code Schengen, en passant par la création d'un corps de garde-frontières européens renforcé, le législateur européen a voulu envoyer un message rassurant aux citoyens européens pour montrer que leur préoccupation relative à l'immigration et au terrorisme n'est pas restée lettre morte¹³²⁵.

Toutefois, la défiance des juristes européens vis-à-vis du PNR n'a pas disparu. Ainsi, pour le Contrôleur européen de la protection des données (CEPD), « le PNR a peu d'utilité pratique, coûte très cher et ses délais très longs de mise en œuvre ne répondent pas aux besoins des forces de l'ordre dans une phase d'urgence »¹³²⁶. Le CEPD a donc écrit dans son avis sur l'accord UE-Canada qu'« à cette date, [il] n'est pas convaincu par les éléments démontrant la nécessité et la proportionnalité du traitement massif et quotidien des données concernant les passagers qui ne sont pas considérés par les services de police comme suspects »¹³²⁷.

Les mêmes controverses ont accompagné l'utilisation de la reconnaissance faciale pour le contrôle d'identité dans les aéroports puisque les droits et les libertés des citoyens français et européens étaient concernés. La CNIL avait à l'époque demandé des garanties solides en matière de protection des données personnelles¹³²⁸ en constatant « une généralisation du recours à des dispositifs biométriques de reconnaissance faciale au sein des aéroports, en France, et particulièrement à l'international ». Elle cita notamment le rapport « Air Transport IT Insights 2018 » de la Société internationale de télécommunication aéronautique (SITA) mentionnant que 63% des compagnies aériennes et 59% des aéroports avaient prévu de déployer des dispositifs de reconnaissance faciale avant 2021¹³²⁹. Les aéroports internationaux

¹³²³ Ibidem

¹³²⁴ J.-P. JACQUE, « Une élection de 'second ordre' ? », *RTD eur.*, 2019, p. 249.

¹³²⁵ Ibidem

¹³²⁶ Coulisses de Bruxelles, 2015, « PNR: un fichier des voyageurs aériens inutile », 21 décembre 2015.

¹³²⁷ Voir : https://edps.europa.eu/sites/edp/files/publication/13-09-30_canada_en.pdf.

¹³²⁸ CNIL, Le « système API-PNR France », Les grands fichiers en fiches, 10 août 2016, en ligne à URL : <https://www.cnil.fr/fr/le-systeme-api-pnr-france> consulté le 10 mai 2023.

¹³²⁹ Ibidem

ont vu dans la reconnaissance faciale un outil leur permettant « d'automatiser les différentes étapes de contrôle » en se substituant aux contrôles de documents d'identité et de voyage¹³³⁰.

La CNIL a pris les enjeux liés à l'introduction de la reconnaissance faciale dans les aéroports avec sérieux puisqu'elle l'a assimilée à un traitement de données particulièrement sensibles qui doit donc faire l'objet d'une protection renforcée. En effet, pour cette autorité administrative indépendante, la technique controversée appartient « à la catégorie plus large des techniques biométriques qui permettent de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, physiologiques ou comportementales »¹³³¹. Dans le RGPD, ces caractéristiques sont qualifiées de « données biométriques » dès lors qu'elles permettent ou visent l'identification unique d'une personne. Elles sont également qualifiées par la CNIL de données « sensibles » au sens de la législation européenne et font l'objet d'un régime juridique spécifique. En principe, leur traitement est interdit et ne peut être mis en œuvre sauf dans certains cas énumérés par le règlement européen en la matière.

Le caractère intrusif de cette technologie « sans contact » inquiète les autorités puisque celle-ci a cette particularité de produire des informations sur le corps de l'individu et le caractérise de façon définitive. Ces données sont uniques et permanentes dans le temps. Le passager ne peut s'en affranchir. Elles accompagnent de plus en plus les passagers dans ce parcours fait de multiples contrôles biométriques dématérialisés. Il existe ainsi un risque que cette technologie alimente un « sentiment d'accoutumance » de la part des passagers, fragilisant les droits et les libertés des citoyens¹³³².

Enjeu à la fois de préservation de la sécurité et de protection des libertés, les dossiers passagers continuent de faire débat. Dans le cadre de la lutte contre le terrorisme, ils servent comme un outil permettant de collecter et d'échanger des données sur les passagers des vols en vue de détecter des terroristes potentiels et de retracer leurs itinéraires. Les attentats de 2015 et de 2016 ont conduit le Conseil européen et le Conseil de l'Union européenne à un changement de ton : la sécurité est plus que jamais une priorité¹³³³. C'est à l'aune de ce contexte que les futurs développements du PNR semblent se faire : la sécurité au détriment des libertés publiques.

¹³³⁰ Ibid.

¹³³¹ Ibid.

¹³³² Ibid.

¹³³³ P. BERTHELET, « Tous les chemins mènent... à Luxembourg, Analyse institutionnelle de l'accord PNR UE-Canada », *RDLF*, chron. n° 20, 2018.

§ 2 – L'ouverture au privé du capital des sociétés aéroportuaires françaises

Historiquement, le statut des aéroports commerciaux français relevait de la loi aéroportuaire de 1933. Ce cadre a été entièrement révisé par la loi n° 2004-809 du 13 août 2004 relative aux libertés et responsabilités locales¹³³⁴ a introduit le transfert aux collectivités territoriales de 150 aérodromes et conservé la compétence de l'État sur ceux qui étaient considérés « d'intérêt national » comme les aéroports d'Aéroports de Paris et les principaux aéroports régionaux (ci-après SAR)¹³³⁵.

Douze mois plus tard, la loi n° 2005-357 du 20 avril 2005¹³³⁶ relative aux aéroports est venue compléter le dispositif en offrant la possibilité d'un transfert des concessions de ces aéroports, dont la liste a été établie par décret, à une société de droit privé. Ladite société dispose d'un capital initial qui est entièrement détenu par des personnes publiques. L'article 7 de cette nouvelle législation, intégrée dans le Code des transports par l'ordonnance n° 2010-1307 du 28 octobre 2010¹³³⁷, fixe les conditions dans lesquelles peuvent être créées les sociétés aéroportuaires régionales. Dorénavant, l'État peut permettre aux collectivités territoriales d'acquérir des participations dans une société à capitaux publics¹³³⁸.

Les SAR ont été créées à Toulouse et Lyon en 2007 et à Nice en 2008 sous la forme de sociétés anonymes à directoire et conseil de surveillance. Elles ont adopté les principes de la gestion privée de manière progressive¹³³⁹. Les personnels ont abandonné leur statut d'agents des Chambres de commerce et d'industrie (CCI) pour un statut de droit commun et les équipes de direction précédentes ont intégré les directoires. Les SAR se sont transformées en des entreprises de taille moyenne, aux côtés des acteurs du développement de leurs territoires, avec des conseils de surveillance constitués de représentants des actionnaires. L'accroissement général du trafic aérien leur est bénéfique. Leur situation financière est généralement équilibrée grâce à des investissements financés par un recours modéré à l'emprunt¹³⁴⁰.

Durant la première décennie du XIX^e siècle, les sociétés aéroportuaires régionales se sont caractérisées par des outils industriels adaptés, avec des infrastructures capables de supporter

¹³³⁴ Loi n° 2004-809 du 13 août 2004 relative aux libertés et responsabilités locales.

¹³³⁵ Cour des comptes, « Le processus de privatisation des aéroports de Toulouse, Lyon et Nice », *Communication à la commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale*, octobre 2018, en ligne à URL <https://www.ccomptes.fr/system/files/2018-11/20181113-processus-privatisation-aeroports-Toulouse-Lyon-Nice.pdf> consulté le 8 mai 2023.

¹³³⁶ Loi n° 2005-357 du 20 avril 2005 relative aux aéroports.

¹³³⁷ Ordonnance n° 2010-1307 du 28 octobre 2010 relative à la partie législative du code des transports.

¹³³⁸ Cour des comptes, op. cit.

¹³³⁹ Ibidem

¹³⁴⁰ Ibid.

un trafic en augmentation. Leur situation économique était saine, car ses sociétés étaient peu endettées et se trouvaient ainsi à même de porter les projets de développement que leurs actionnaires allaient définir. Les crises financières et les attentats terroristes ont créé un contexte international qui a pu ralentir momentanément la croissance du secteur aérien. Toutefois, les perspectives du développement sur le long terme n'ont pas été infirmées. Par ailleurs, la baisse durable des taux d'intérêt a incité les principaux acteurs à un redémarrage et une accélération de la demande¹³⁴¹.

Au début de la deuxième décennie de ce siècle, et avant la crise du Covid-19, le secteur aérien a vu se développer une sérieuse concurrence entre les plateformes aériennes, notamment les plus grandes d'entre elles, tant au niveau international qu'européen et national¹³⁴². Ces aéroports se distinguent par une industrie à coûts fixes, une forte intensité capitalistique. Ces plateformes sont entrées dans une logique financière exigeant d'attirer de nouveaux acteurs avec des compagnies aériennes capables d'ouvrir de nouvelles lignes pour une demande croissante vers de nouvelles destinations. Dans ce contexte, les aéroports métropolitains se sont révélés être des investissements sans grands risques à court, moyen et long terme compte tenu des perspectives favorables du trafic aérien et de la conjoncture économique internationale. Cette situation ne se limite pas au cas français puisque les analystes de la Commission européenne¹³⁴³ considèrent que, sauf circonstances exceptionnelles telles que les pandémies par exemple, les aéroports recevant plus de 5 millions de passagers sont structurellement à même de couvrir la totalité de leurs coûts et confirment ainsi leur rentabilité.

C'est dans ce contexte que les sociétés aéroportuaires de Lyon, Nice et Toulouse ont été privatisées et valorisées à des degrés supérieurs aux attentes de l'État actionnaire, puisque les cessions de parts ont été réalisées dans un cadre juridique qui a permis de garantir l'intérêt financier de l'État tout en prenant en compte la dimension industrielle de chaque projet.

Toutefois, des interrogations demeurent quant à la capacité de ces aérodromes à garantir des gains d'efficience avec l'arrivée de nouveaux acteurs économiques et d'être à même de compenser une demande de rémunération accrue. Recentré sur ses fonctions de régulateur et de concessionnaire, l'État français voit un autre défi se poser avec les privatisations puisque l'efficacité de ses moyens de contrôle, dans un contexte de finances publiques tendu, est mise

¹³⁴¹ Ibid.

¹³⁴² P. CHIAMBARETTO & E. COMBE, « V / Les défis à venir du transport aérien », in Paul Chiambaretto (dir.), *Le transport aérien*, La Découverte, 2023, pp. 99-118.

¹³⁴³ Rapport sur le maillage aéroportuaire français au Conseil supérieur de l'aviation civile, 2016.

à l'épreuve. Pour la Cour de comptes, l'arsenal législatif étatique devra « en tout état de cause être consolidé afin de pouvoir pleinement jouer son rôle et permettre une juste répartition des profits entre les différents acteurs du transport aérien »¹³⁴⁴.

§ 3 – Le projet de privatisation controversé de la société Aéroports de Paris

La privatisation des Aéroports de Paris a été longuement commenté dans la presse française. Longtemps resté à l'état de projet depuis le transfert partiel des participations publiques à l'acteur privé en 2006, le processus de privatisation d'ADP a finalement été initié dans les années 2010¹³⁴⁵. La réalisation d'une telle opération n'est devenue que plus aisée depuis la privatisation des sociétés aéroportuaires de Nice, Toulouse et Lyon¹³⁴⁶. Il revenait toutefois au législateur d'en préciser le mode juridique de l'opération¹³⁴⁷. Les promoteurs du projet de loi aspiraient à modifier le régime juridique applicable à ADP, à limiter la durée d'exploitation de la plateforme parisienne à 70 ans et à prévoir le transfert des biens appartenant aux aéroports parisiens à l'État lorsque l'exploitation prendra fin. À l'époque, ADP avait le droit d'exploiter indéfiniment les infrastructures aéroportuaires, depuis les réformes de 2005.

La crise du coronavirus à partir de 2019 est venue bouleverser ce projet puisque le secteur aérien a souffert des difficultés des transporteurs et des compagnies aériennes. Les aéroports ont dû subir des mesures de confinement, la prudence des voyageurs et des annulations de voyages personnels et professionnels¹³⁴⁸. En 2020, la crise sanitaire globale a porté un coup d'arrêt au mouvement aérien pourtant bien en hausse en 2019, avec un chiffre record de plus de deux millions de passagers ayant utilisé les plateformes aériennes. Les flux d'avions commerciaux, le fret commercial, le trafic de La Poste et le trafic de passagers ont été affectés par cette crise et ont connu une baisse significative. Le trafic international, fortement impacté,

¹³⁴⁴ Cour des comptes, « Le processus de privatisation des aéroports de Toulouse, Lyon et Nice », Communication à la commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale, octobre 2018, en ligne à URL : <https://www.ccomptes.fr/system/files/2018-11/20181113-processus-privatisation-aeroports-Toulouse-Lyon-Nice.pdf> consulté le 8 mai 2023.

¹³⁴⁵ Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises.

¹³⁴⁶ La loi n° 2005-357 du 20 avril 2005 sur les aéroports a permis à ces trois aéroports de se constituer en sociétés aéroportuaires régionales (SAR). Ces sociétés anonymes avaient un capital initialement réparti entre l'État (60 %), la chambre de commerce et d'industrie (25 %), et les collectivités territoriales (15 %). Les trois aéroports concernés ont adopté ce statut en 2007 et 2008.

¹³⁴⁷ L'État a successivement engagé des procédures de cession de ses participations dans les sociétés aéroportuaires régionales (SAR) de Toulouse en 2014, conformément à la loi n° 86-912 du 6 août 1986 sur les privatisations, ainsi qu'à l'ordonnance n° 2014-948 du 20 août 2014 sur la gouvernance des sociétés à participation publique. Les cessions des participations dans les SAR de Lyon et Nice ont suivi en 2016, dans le cadre de cette même ordonnance, complétée par la loi n° 2015-990 du 6 août 2015 pour la croissance et l'activité.

¹³⁴⁸ Rédaction, « Aéroports de Paris : pas de référendum, mais un report de la privatisation », *France 24*, 12 mars 2020, en ligne à URL : <https://www.france24.com/fr/20200312-a%C3%A9roports-de-paris-pas-de-r%C3%A9f%C3%A9rendum-mais-un-report-de-la-privatisation> consulté le 22 avril 2023.

a chuté de plus de deux tiers¹³⁴⁹. Ainsi, au cours de l'année 2020, le trafic, toutes destinations réunies pour les passagers nationaux, hors transit, était inférieur de moitié à celui de l'année 2019 durant la même période : 991 205 passagers locaux transportés en 2020 contre 1 971 655 en 2019. Le trafic total de passagers a donc fléchi de 50,1 % par rapport à l'année précédente, à la suite de l'évolution détériorée du trafic transit avec une baisse d'au moins 60 %¹³⁵⁰.

L'entité Aéroports de Paris était un établissement public¹³⁵¹ que le gouvernement français a transformé, en 2005, en société anonyme¹³⁵². Cette dernière a ensuite été introduite en bourse en 2006¹³⁵³. Pour autant, l'article 6323-1 du Code des transports¹³⁵⁴ imposait à l'État de détenir la majorité de son capital. Ainsi, en juillet 2018, l'État français détenait 50,6 % des parts. Le cadre légal a dû donc être modifié pour qu'un projet de privatisation soit possible¹³⁵⁵. D'autres sociétés ont des participations dans le capital de la société Aéroports de Paris, c'est le cas notamment des groupes Schiphol, gérant de l'aéroport d'Amsterdam, et Vinci, qui détiennent chacun une participation de 8 %¹³⁵⁶.

La société Aéroports de Paris se trouve à la tête du Groupe ADP qui disposent de filiales œuvrant dans les domaines de l'ingénierie, de la gestion et du développement aéroportuaires, en France et à l'étranger. Diversifiant ses activités, la société s'investit dans la gestion immobilière et la gestion de commerces et de services dans l'espace des aéroports parisiens. La société aéroportuaire parisienne détient la propriété et exploite les principaux aéroports de la région, notamment Charles de Gaulle (ci-après CDG), Orly et Le Bourget¹³⁵⁷.

Les principales recettes que tire la société viennent des redevances prélevées sur les passagers et sur les compagnies aériennes, issues notamment des atterrissages, du stationnement des avions, de services comme le tri des bagages. Elle reçoit également des redevances (d'un montant de 0,5 Md€ au titre de la taxe d'aéroport en 2017), pour financer certaines mesures

¹³⁴⁹ J. JEAN-MARIE, « Transport aérien - La crise sanitaire porte un coup d'arrêt au trafic aérien INSEE », *Conjoncture Martinique*, n° 14, 08 juillet 2021.

¹³⁵⁰ Ibidem

¹³⁵¹ Avant la modification apportée par la loi n° 2005-357 relative aux aéroports du 21 avril 2005, la société ADP était un établissement public de droit français doté de l'autonomie financière en vertu de l'article L. 251-2 du code de l'aviation civile français (abrogé par l'ordonnance n° 2010-1307 du 28 octobre 2010 relative à la partie législative du code des transports).

¹³⁵² La loi n° 2005-357 du 20 avril 2005 a transformé ADP, ancien établissement public, en société. Cette loi lui a confié la gestion et le développement des aérodromes d'Île-de-France, dont Paris-Charles-de-Gaulle et Paris-Orly (C. transp., art. L. 6323-2).

¹³⁵³ Cette décision s'inscrit dans le cadre de la loi n° 2005-357 du 20 avril 2005.

¹³⁵⁴ Code des transports, article 6323-1.

¹³⁵⁵ La loi n° 2019-486 du 22 mai 2019, dite « loi PACTE », a autorisé la privatisation du capital de cette société.

¹³⁵⁶ F. ECALLE, « Les enjeux de la privatisation des aéroports de Paris », *Les commentaires de l'actualité, FIPECO*, 3 septembre 2018.

¹³⁵⁷ Ibidem

de sûreté comme le filtrage de passagers qui implique l'utilisation des données à caractère personnel des passagers¹³⁵⁸.

Un contrat de régulation économique (ci-après CRE) avec l'État encadre les redevances aéronautiques en fixant leur augmentation annuelle maximale. L'Autorité de supervision indépendante des redevances aéroportuaires homologue chaque année le barème des redevances dans le respect des plafonds que le contrat mentionné ci-dessus fixe¹³⁵⁹.

La polémique sur la privatisation d'ADP a commencé en décembre 2017 lorsque la Bank of America-Merrill Lynch a été mandatée par l'Agence des participations de l'État (APE) pour gérer le dossier de privatisation¹³⁶⁰. Le 18 juin 2018, le projet de loi relatif au plan d'action pour la croissance et la transformation des entreprises (PACTE) a été présenté en Conseil des ministres et prévoyait la privatisation de la société Aéroports de Paris¹³⁶¹. Le Conseil constitutionnel a validé le 9 mai 2019 les dispositions prévoyant cette privatisation¹³⁶². 250 députés et sénateurs de divers partis d'opposition se sont mobilisés pour obtenir le premier référendum d'initiative partagée (RIP). Toutefois, le nombre de signatures requis, 10% du corps électoral, n'a pas été atteint¹³⁶³. La crise économique causée par la pandémie du Covid-19 et la chute des cours du pétrole ont créé un contexte défavorable au projet de cession de la société Aéroports de Paris¹³⁶⁴.

Cela étant, le débat sur cette privatisation ne disparaîtra pas facilement sachant que depuis 2006¹³⁶⁵, les autorités françaises se sont engagées vis-à-vis de la Commission européenne à mettre en œuvre une procédure d'appel d'offres, sur la base d'un cahier des charges, pour répondre à la nécessité de mettre en concurrence le plus grand nombre d'investisseurs répondant à « des modalités ouvertes, transparentes et non discriminatoires »¹³⁶⁶. Cette action

¹³⁵⁸ Ibid.

¹³⁵⁹ Ibid.

¹³⁶⁰ B. BAYART, « Aéroports de Paris : l'État prépare la privatisation », *Le Figaro*, 8 décembre 2017, en ligne à URL : <https://www.lefigaro.fr/societes/2017/12/08/20005-20171208ARTFIG00289-aeroports-de-paris-l-etat-prepare-la-privatisation.php> consulté le 8 mai 2023.

¹³⁶¹ F. ECALLE, « Les enjeux de la privatisation des aéroports de Paris », *Les commentaires de l'actualité, FIPECO*, 3 septembre 2018.

¹³⁶² Conseil constitutionnel, décision n° 2019-781 DC du 16 mai 2019 concernant la loi relative à la croissance et la transformation des entreprises

¹³⁶³ Rédaction, « Aéroports de Paris : pas de référendum, mais un report de la privatisation », *France 24*, 12 mars 2020, en ligne à URL : <https://www.france24.com/fr/20200312-a%C3%A9roports-de-paris-pas-de-r%C3%A9f%C3%A9rendum-mais-un-report-de-la-privatisation> consulté le 8 mai 2023.

¹³⁶⁴ S. NICINSKI, « La privatisation et le statut d'Aéroports de Paris », *Lextenso, Revue du droit public*, n° 2, mars 2021, p. 389.

¹³⁶⁵ Sur les conditions de l'ouverture du capital de la société, lire l'avis n° 2006-A-4 du 13 juin 2006 de la Commission des participations et des transferts relatif à l'ouverture minoritaire du capital de Aéroports de Paris.

¹³⁶⁶ Cour des comptes, « Le processus de privatisation des aéroports de Toulouse, Lyon et Nice », Communication à la commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée

encouragerait ainsi un environnement concurrentiel fort. Par ailleurs, cette procédure a l'avantage de faciliter l'association des collectivités locales.

Sous-section 2 – La protection des données personnelles des passagers aériens face à la privatisation des aéroports

La privatisation des aéroports soulève des défis juridiques du fait, notamment, du développement incessant du secteur aérien. La multiplication des échanges et l'accès grandissant au tourisme de masse a engendré une croissance vertigineuse du nombre d'utilisateurs du transport aérien. La CNIL a ainsi rappelé que 100 000 passagers par an et 230 compagnies sont concernés par le système API PNR en France¹³⁶⁷. Bien que les Aéroports de Paris n'aient pas été privatisés, le groupe en charge de ces derniers a déjà pris en compte l'ampleur des défis en termes de protection des données à caractère personnel des passagers aériens.

§1 – Les usagers du transport aérien face au développement croissant de la privatisation du secteur aéroportuaire

La montée en puissance du mouvement de privatisation dans le secteur aéroportuaire est désormais un fait. Que ce soit en tant que prestataire, occupant ou gestionnaire, le « secteur privé » tend à remplacer le « secteur public » dans l'environnement juridique français. La transition des institutions publiques vers des sociétés commerciales en tant que modèle de gestion a permis l'émergence des opérations en capital. Il est alors fréquent qu'un investisseur privé fasse son entrée, en peu de temps, dans le capital des sociétés françaises d'exploitation aéroportuaire, attiré par des marges de bénéfices élevées. Bien qu'une partie du processus de libéralisation du marché du transport aérien ait été initiée au niveau européen et semble donc s'imposer, l'ouverture du capital de ces compagnies à de tels acteurs ne se fait pas sans une certaine réticence des acteurs publics et des usagers¹³⁶⁸.

Méfiant à l'idée de confier la gestion des aéroports de France à des sociétés privées dont les ambitions, selon les détracteurs, ne peuvent satisfaire que la seule demande de leurs actionnaires, les usagers du transport aérien n'ont pas caché leurs inquiétudes face à ces projets de privatisation annoncés. Après la première tentative d'ouverture du capital de la

nationale, octobre 2018, en ligne à URL : <https://www.ccomptes.fr/system/files/2018-11/20181113-processus-privatisation-aeroports-Toulouse-Lyon-Nice.pdf> consulté le 8 mai 2023.

¹³⁶⁷ CNIL, Le « système API-PNR France », Les grands fichiers en fiches, 10 août 2016, en ligne à URL : <https://www.cnil.fr/fr/le-systeme-api-pnr-france> consulté le 10 mai 2023.

¹³⁶⁸ S. PARIER, « Les incidences de la privatisation sur les usagers : entre faux-semblants et réalités », *Juris tourisme*, Tourisme & territoire, Aéroports, Dalloz, n° 206, 2018, p. 35.

société gestionnaire des aéroports de Paris, les gouvernements français ont voulu rattraper le retard par rapport à leurs voisins européens en se lançant dans une campagne plus globale de privatisation. C'est dans ce contexte que l'État, à partir de 2015, a cédé partiellement sa participation dans la société d'exploitation de l'aéroport de Toulouse-Blagnac, avant d'accepter une cession intégrale de sa participation dans la structure qui gère les aéroports de Nice et de Lyon¹³⁶⁹.

Cependant, si l'État entend privatiser les structures de gestion des plus grandes plateformes aéroportuaires dont il est actionnaire, il n'entend pas céder au secteur privé la propriété des terrains sur lesquels sont implantés ces aéroports. En effet, il apparaît que le processus de privatisation de ces dernières années ne concerne que le capital de la société aéroportuaire et non les domaines concédés par les autorités publiques à la plateforme d'exploitation de la société aéroportuaire. Dès lors, bien qu'un acteur privé ne puisse pas être entièrement propriétaire de l'aéroport, force est de constater que cette évolution suscite des interrogations, voire des inquiétudes chez les utilisateurs de ces plateformes, « qu'il s'agisse de la question de l'exploitation qui sera mise en œuvre par le gestionnaire privatisé ou de celle relative à la qualité et au prix du service public qui leur sera rendu »¹³⁷⁰.

D'un point de vue juridique, la privatisation entraîne le transfert du contrôle du capital et du pouvoir de décision à des investisseurs privés sur la base de la majorité des droits de vote aux assemblées d'actionnaires¹³⁷¹. Conséquence logique de la détention d'un tel capital, la société exploitante ne pourrait plus revendiquer le statut d'entreprise publique dont la personnalité juridique serait désormais contrôlée par des investisseurs privés, fort probablement amenés à appliquer un certain libéralisme. Dans la logique du libre marché, les acteurs privés attendent un retour sur leur investissement et une telle ambition n'est pas nécessairement compatible avec la satisfaction des besoins attachés à un bien collectif. Toutefois, à ce jour, l'État gère de plus en plus son actionnariat à la manière d'un actionnaire privé, notamment avec l'aide d'un organe étatique actionnaire chargé de veiller aux intérêts patrimoniaux de l'État et plus largement aux intérêts des actionnaires. Dès lors, la gestion de l'aéroport par un acteur privé n'est pas forcément moins bonne que celle de l'État actionnaire comme la privatisation des aéroports français ne signifiera pas inévitablement que les considérations d'intérêt général seront reléguées au second plan.

¹³⁶⁹ Ibidem

¹³⁷⁰ Ibid.

¹³⁷¹ P. DELVOLVÉ, « La privatisation du service de l'État », *Pouvoirs*, vol. 117, n° 2, 2006, pp. 107-120.

Pour Simon Parier¹³⁷², il n'est pas certain que la logique mercantile, qui est certainement plus importante dans les entreprises à capitaux privés que dans les entreprises à capitaux publics, se traduise par la mise en œuvre d'une stratégie commerciale purement axée sur la maximisation du profit des actionnaires. Au contraire, selon les juristes, à terme, cette logique peut mieux répondre aux besoins des usagers des aéroports parmi lesquels figurent évidemment les touristes de passage. Les différents projets annoncés par le cessionnaire après la prise de contrôle, l'agrandissement et la rénovation des infrastructures pour faciliter l'accueil et le transit des passagers, ou encore le développement de la partie commerciale de l'aéroport pour répondre à de nouveaux besoins suffisent à montrer que la privatisation des aéroports ne nuira pas nécessairement aux utilisateurs publics du service.

Cependant, les préoccupations des usagers ne se résument pas à la gestion de la plateforme aéroportuaire mais concernent également la qualité des services publics que les opérateurs privés fourniront et l'éventuelle augmentation des redevances qui leur seront facturées après la privatisation.

Toutefois, l'évolution de la répartition du capital des sociétés d'exploitation aéroportuaire ne remet pas en cause leur modèle de gestion. Ainsi, toutes les composantes du système de concession de service public seraient maintenues. Le système, basé sur des contrats et des normes standards, permet à l'État de conserver une influence significative dans la gestion des aéroports privatisés en tant que concédant et donc garant des intérêts collectifs et des droits d'usage. Ainsi, écartant le spectre d'une gestion entièrement axée sur le profit, la privatisation¹³⁷³ ne décharge en rien les opérateurs de leurs obligations vis-à-vis des usagers.

Le gestionnaire de ce type d'aéroport privatisé reste lié par toutes une série d'obligations prévues par le contrat et le cahier de charges, jusqu'à la fin de la période de concession convenue. Par conséquent, l'exploitant privatisé doit s'assurer du plein respect de l'objet de la concession, de la réglementation spécifique liée à l'exploitation du service objet de la délégation et des règles économiques et financières spécifiques, comme la tarification des services offerts. La privatisation n'introduisant aucun changement en matière de franchise, l'utilisateur ne doit pas voir la qualité des services qui lui sont proposés affectée par cette évolution. L'élaboration d'un cahier des charges type est vu comme la référence s'agissant des droits de l'utilisateur aéroportuaire. Ce texte peut prévoir un possible retrait de l'État mais ses

¹³⁷² S. PARIER, « Les incidences de la privatisation sur les usagers : entre faux-semblants et réalités », *Juris tourisme*, Tourisme & territoire, Aéroports, Dalloz, n° 206, 2018, p. 35.

¹³⁷³ S. PARIER, « Privatisation : un projet « révolutionnaire » ? », *Juris Tourisme*, Tourisme & territoire, Aéroports de Paris, Dalloz, n° 214, 2018, p. 35.

rédauteurs peuvent dresser une description détaillée de la mission de service public à préserver, des conditions de son exécution et des moyens de contrôle. Le service public rendu à l'utilisateur est *a priori* réalisé dans les mêmes conditions qu'antérieurement à la privatisation. Toutefois, l'enjeu de la privatisation réside, pour les usagers, dans le fait de savoir s'il sera rendu au même prix. À défaut, les craintes de celles et ceux qui se sont préoccupés des projets de privatisation auront été fondées¹³⁷⁴.

En contrepartie de l'utilisation de ces installations aéroportuaires et des services rendus, le concessionnaire obtient le droit de percevoir des redevances des usagers. Toutefois, ce droit ne l'autorise pas à arrêter seul le montant de manière discrétionnaire¹³⁷⁵. En effet, ces redevances doivent être fixées, à l'issue d'une procédure stricte, en tenant compte, de manière raisonnable, du coût total des installations et des services qu'elles ont pour but de rémunérer. L'instauration de ces redevances est soumise en principe à plusieurs contrôles sous l'égide de l'Autorité de supervision indépendante (ASI). Nonobstant l'arsenal juridique instauré pour éviter les abus de gestionnaire, les usagers ont exprimé leurs préoccupations vis-à-vis d'une possible augmentation des tarifs aéroportuaires après l'ouverture du capital des plateformes en France, puisque l'établissement du montant des redevances est, dans un contexte de forte concurrence, une inquiétude majeure des acteurs du milieu aéroportuaire. Lesdites redevances, tout en étant versées par les compagnies aériennes aux gestionnaires, sont répercutées sur les prix des billets achetés par les passagers aériens qui assument ainsi en définitif le prix global. Une évolution des modes de régulation, ou la prise de participation de groupe de BTP, peut constituer une hausse effective des niveaux de redevance. Ce risque avait été souligné par l'Autorité de concurrence dans les débats selon Simon Parier¹³⁷⁶. Des engagements ont été pris pour veiller au contrôle de l'évolution de ces prix. Ces prises de position ont pour objectif d'éviter aux usagers des plateformes de subir des inconvénients à la suite d'un processus de privatisation mais il ne pourra éviter le passage de son statut d'utilisateur de service public à client.

¹³⁷⁴ S. PARIER, « Les incidences de la privatisation sur les usagers : entre faux-semblants et réalités », *Juris tourisme*, Tourisme & territoire, Aéroports, Dalloz, n° 206, 2018, p. 35.

¹³⁷⁵ Ibidem

¹³⁷⁶ Ibid.

§ 2 – Le volontarisme européen en matière de respect des droits fondamentaux illustré par la politique de protection des données personnelles des Aéroports de Paris

En 2020¹³⁷⁷, le groupe Aéroports de Paris a publié sa politique de protection des données à caractère personnel dont le but est de définir ses engagements en matière de protection desdites données, notamment vis-à-vis de ses parties prenantes qui incluent les salariés, les clients et les partenaires, affichant ainsi sa volonté de se conformer au cadre légal en vigueur, en particulier au RGPD. Une organisation a été mise en place à cet effet et la politique du groupe vise à mettre en avant des principes ainsi que des règles à même de garantir une protection adéquate des données utilisées dans le cadre des activités du groupe.

Le RGPD indique que la protection de ces données personnelles nécessite de prendre des mesures techniques et organisationnelles appropriées dans le but de garantir un niveau de sécurité adapté aux risques associés à la sécurité des données. L'article 32 de ce règlement impose cette obligation tant au responsable du traitement qu'aux sous-traitants impliqués¹³⁷⁸. Cet article énumère les mesures techniques et organisationnelles à mettre en place par l'organisme afin de garantir la sécurité des données et leur utilisation. En France, plusieurs décisions de la CNIL relatives à l'article 32 du RGPD semblent indiquer que cette dernière souhaite mettre fin à la négligence fréquente des entreprises en matière de sécurité du traitement des données¹³⁷⁹.

Au-delà des enjeux de conformité juridique, le groupe s'est chargé « d'assurer la confiance des personnes concernées dont les données sont utilisées, en évitant leur vol, leur modification non désirée ou leur destruction involontaire et toute atteinte à la vie privée qui pourrait résulter de telles violations de données »¹³⁸⁰, montrant ainsi qu'en Europe, et même parfois aux États-Unis, les acteurs économiques ont saisi l'importance pour l'opinion publique du respect des droits fondamentaux en lien avec la vie privée. Dans le cas contraire, il peut y avoir un impact sur l'image de leur entreprise et *in fine* sur la crédibilité des services qu'ils proposent.

Cette politique a été adoptée par la société Aéroports de Paris et ses entités auxquelles elle applique un contrôle exclusif, directement et indirectement, et qui sont basées dans l'espace

¹³⁷⁷ Groupe ADP, « Politique Groupe de Protection des Données à caractère personnel », 12 novembre 2020, en ligne à URL : <https://www.parisaeroport.fr/docs/default-source/groupe-fichiers/rse/group-personal-data-protection-policy---french-version-only.pdf> consulté le 11 mai 2023.

¹³⁷⁸ RGPD, article 32.

¹³⁷⁹ CNIL, délibération SAN-2022-009 du 15 avril 2022 ; délibération SAN-2021-019 du 29 octobre 2021 ; délibération SAN-2021-008 du 14 juin 2021.

¹³⁸⁰ Groupe ADP, op. cit.

de l'Union européenne. Les salariés de ces « société(s) concernée(s) », comme les mentionne le document commenté, tout comme les intervenants extérieurs coopérant avec le groupe ADP, sont les destinataires de cette politique. Cette dernière concerne tout type de traitement, numérique ou non, effectué par les « sociétés concernées » du groupe, que ce soit pour son compte ou pour celui d'un client, avec l'aide ou non d'un prestataire¹³⁸¹.

Cette politique de protection des données personnelles est conçue en complément d'autres documents du groupe dont la Politique Groupe de Protection de l'Information (PGPI) qui concerne tout type d'information et la Politique de Sécurité du Système d'Information (PSSI) qui couvre les systèmes informatiques qui traitent ces informations.

Traitant différents types de données, celles de ses salariés comme celles des passagers, des clients, des fournisseurs ou toute autre catégorie de parties, les sociétés du groupe ADP doivent respecter la législation de leur pays, le RGPD et les lois européennes spéciales comme la directive sur le PNR, en plus d'autres lois sectorielles comme le Code de la santé publique en France.

Un aéroport comme celui d'Orly, par exemple, doit ainsi respecter les principes fondamentaux de protection des données suivants¹³⁸² : tout traitement de données à caractère personnel doit être légitime (sa finalité doit être précise, justifiée et déclarée dans un registre des traitements) ; les données manipulées dans le cadre d'un traitement doivent être limitées à celles strictement nécessaires à la réalisation de la finalité de ce traitement, aucune autre action que celles décrites au registre ne doit être réalisée avec ces données ; les durées de conservation des données doivent être définies (elles doivent être proportionnées à la finalité du traitement et respecter les obligations légales applicables à l'activité) ; la confidentialité, l'intégrité et la disponibilité des données doivent être garanties par la mise en œuvre de mesures de sécurité adaptées aux risques pour la personne que pourraient engendrer un accès illégitime, une modification impromptue ou une perte de ses données, ces mesures doivent respecter les politiques de protection de l'information et de sécurité des systèmes d'information du Groupe ADP et les droits des personnes dont les données sont manipulées doivent être respectés (lesdites personnes doivent être clairement informées de l'utilisation de leurs données et recevoir une réponse à toute demande relative à leurs données dans les meilleurs délais et en moins d'un mois maximum). Or, on a pu remarquer sur le site de l'aéroport d'Orly que les passagers n'ont pas un accès clair et direct à ces informations,

¹³⁸¹ Ibidem

¹³⁸² Ibid.

notamment lorsqu'il est question des « formalités de voyage », du « contrôle du passeport » et du « passage frontière »¹³⁸³.

Dans ce cadre juridique, plusieurs mesures ont toutefois été prises par le groupe ADP pour assurer la protection des données à caractère personnel¹³⁸⁴. Tout d'abord, un responsable de traitement a pour mission de garantir, en tant que responsable légal, la conformité de la société avec le droit en vigueur. En tant que responsable de traitement, il doit fournir à ses collaborateurs les moyens d'assurer la protection des données personnelles des passagers aériens de façon proportionnée aux risques et pouvoir démontrer aux autorités de contrôle la conformité des traitements desdites données qui sont réalisés dans le cadre de ses activités. Ce responsable effectue les arbitrages nécessaires en cas d'écart entre les exigences opérationnelles et réglementaires. Il peut aussi déléguer ses missions à ses directeurs.

De plus, un délégué à la protection des données (ci-après DPD) est désigné dans chaque société concernée du groupe ADP. Le DPD a pour obligations principales d'informer le responsable de traitement et l'ensemble des collaborateurs de l'entreprise des obligations qui leur incombent ainsi que de les conseiller dans leur mise en œuvre. Il est sollicité, en particulier, lors des analyses d'impact sur la vie privée qui sont nécessaires à la mise en conformité des traitements sensibles vis-à-vis du RGPD, pour contrôler le respect des réglementations sur la protection des données et enfin pour assurer la coopération avec l'autorité de contrôle¹³⁸⁵.

Chaque salarié du groupe ADP¹³⁸⁶ a, en outre, l'obligation de connaître les règles de protection des données à caractère personnel et de les appliquer, c'est pourquoi une charte d'application des exigences sur lesdites règles est diffusée et applicable aux collaborateurs. C'est en particulier le cas pour les managers, responsables d'activités et chef de projets qui doivent étudier les obligations de protection des données personnelles sur leur périmètre de responsabilité et s'assurer que leurs équipes sont en conformité avec la politique du groupe. Les collaborateurs du groupe doivent s'assurer de la prise en compte des exigences de protection des données dès la mise en place d'un nouveau projet ou l'évolution d'un système existant, en s'appuyant sur des conseils juridiques ainsi que des experts en informatique et en protection des données.

¹³⁸³ Orly Facile, « Formalités voyages », *Aéroport Orly*, 2023, en ligne à URL : <https://www.orly-aeroport.fr/formalites-voyage/> consulté le 12 mai 2023.

¹³⁸⁴ Groupe ADP, « Politique Groupe de Protection des Données à caractère personnel », *Aéroports de Paris*, 12 novembre 2020, en ligne à URL : <https://www.parisaeroport.fr/docs/default-source/groupe-fichiers/rse/group-personal-data-protection-policy---french-version-only.pdf> consulté le 11 mai 2023.

¹³⁸⁵ Ibidem

¹³⁸⁶ Ibid.

Un comité de protection des données à caractère personnel se réunit deux à trois fois par an¹³⁸⁷. Ce comité supervise et coordonne les efforts de mise en conformité des différentes entités du groupe Aéroport de Paris. Il est dirigé par le délégué à la protection des données de la société mère. Le comité comprend également des délégués à la protection des données de chaque société concernée, le responsable du management des risques du groupe, ainsi qu'un représentant désigné de la direction juridique d'ADP. Si l'ordre du jour l'exige, le responsable de la sécurité des systèmes d'information du groupe peut également être invité à participer.

Ce document sur la politique du groupe ADP ne mentionne pas explicitement la directive européenne sur le PNR. Or, ce cadre normatif européen fournit aux autorités de contrôle nationales les instruments et les mécanismes nécessaires pour garantir les droits au respect de la vie privée et à la protection des données à caractère personnel des passagers aériens. Il est essentiel que la politique du groupe ADP mentionne les régimes juridiques applicables à tous les acteurs destinataires des données personnelles des dossiers passagers, notamment les gouvernements nationaux, les autorités répressives, les services chargés de la protection des données à caractère personnel ainsi que les responsables du traitement des données et les personnes concernées¹³⁸⁸.

Pour mieux comprendre les défis auxquels l'Union européenne est confrontée en matière de protection juridique des données à caractère personnel, il est essentiel de considérer la complexité de la mise en œuvre d'un système PNR, exacerbée par la diversité des compétences des services répressifs selon la législation nationale des États membres. La mise en œuvre d'un système PNR dans l'espace de l'Union européenne est rendue encore plus complexe par la diversité des compétences des services répressifs en fonction de la législation nationale des États membres, incluant ou non l'immigration, le renseignement, les missions de police, les intervenants privés ou la fiscalité¹³⁸⁹. C'est ce qu'a rappelé le Contrôleur européen de la protection des données dans un avis rendu le 1^{er} mai 2008 sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers à des fins répressives.

¹³⁸⁷ Ibid.

¹³⁸⁸ Avis du Contrôleur européen de la protection des données du 1^{er} mai 2008 sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives (JOUE n° C 110, 1^{er} mai 2008).

¹³⁸⁹ Ibidem.

§ 3 – *La privatisation des aéroports dans l’environnement juridique entremêlé d’interconnexion des fichiers et de sécurité numérique*

La volonté d’ouvrir les capitaux des sociétés aéroportuaires à des acteurs privés, qui s’est accentuée ces deux dernières décennies, intervient dans un cadre caractérisé par divers défis, d’ordre technique et sécuritaire. Au sein des pays de l’Union européenne, des pays comme la France, la Belgique et l’Autriche ont été victimes d’attaques terroristes, notamment en 2015 et 2016, en plus de devoir gérer les tensions liées à la crise migratoire. Les États membres, par la voix du Conseil européen et du Conseil de l’UE, ont décidé que la politique à suivre était de sécuriser davantage les frontières extérieures de l’Union européenne¹³⁹⁰.

En droit international, les résolutions du Conseil de sécurité des Nations-Unies avaient déjà prévu l’utilisation des données personnelles des passagers aériens dans le cadre de la gestion des frontières pour lutter notamment contre les projets d’attentats terroristes. Les membres du Conseil de sécurité ont en effet voté, le 21 décembre 2017, la résolution 2396 dans laquelle il était demandé aux États membres de collecter les données des passagers aériens pour empêcher le retour des combattants terroristes étrangers. Le Conseil de sécurité a ainsi explicitement « exhort[é] les États membres à envisager, le cas échéant, de déclasser à des fins administratives les données de renseignement, y compris les données relatives aux voyages (...) afin de communiquer (...) et de les transmettre comme il convient aux autres États et organisations internationales compétentes concernés (...) »¹³⁹¹. Le contrôle des dossiers passagers a été conçu pour tracer les déplacements des individus suspects afin de lutter contre ceux qui sont susceptibles de commettre un acte terroriste. Le recours à des fichiers est devenu, au fil du temps, une pratique courante, surtout depuis l’entrée de l’informatique dans le système aéroportuaire avec des capacités quasiment illimitées d’exploitation et de croisement des données à caractère personnel des passagers aériens.

En matière de politique migratoire de l’Union européenne, de nouvelles règles visant à traiter la porosité des frontières sont devenues l’un des enjeux majeurs de la lutte contre le terrorisme. La communication de la Commission européenne du 6 avril 2016 en atteste¹³⁹². Intitulée « Des systèmes d’information plus forts et plus intelligents pour les frontières et la

¹³⁹⁰ P. BERTHELET, « La sécurité digitale à l’heure des crises migratoire et terroriste, le nœud gordien de l’interconnexion des fichiers », *GDR ELSJ*, 20 avril 2016, en ligne à URL : <http://www.gdr-elsj.eu/2016/04/20/cooperation-judiciaire-penale/la-securite-digitale-a-lheure-des-crisis-migratoire-et-terroriste-le-noeud-gordien-de-linterconnexion-des-fichiers/#more-4794> consulté le 17 mai 2023.

¹³⁹¹ Conseil de sécurité, Résolution 2396 (2017), ONU.

¹³⁹² European commission, “Stronger and Smarter Information Systems for Borders and Security”, Communication from the Commission to the European Parliament and the Council, COM(2016) 205 final, Brussels, 6 April 2016.

sécurité », ce texte affirme sans détours une « interconnexion dynamique » entre migration, police et gestion des frontières. À cette époque, la crainte principale était le phénomène des combattants de l'État islamique venant d'Irak et de Syrie, notamment ceux que l'on appelait les « revenants » et qui projetaient de commettre des attentats terroristes sur le sol européen¹³⁹³. Certains ont participé aux attentats terroristes qui ont endeuillé la France¹³⁹⁴.

Depuis plusieurs années, l'Union européenne tente d'endiguer ce phénomène des combattants étrangers en développant deux axes : d'une part, l'interconnexion et la synergie des systèmes d'information dans le but de garantir les vérifications systématiques, portant respectivement sur les personnes et les documents ; d'autre part, l'équipement des postes en matériels plus performants – capables, par exemple, de lire vite et de manière fiable les pistes magnétiques des documents de voyage présentés au garde-frontière – et leur connexion aux bases de données centrales internationales, européennes et nationales pour permettre que soient données de promptes réponses aux requêtes informatiques des agents employés au contrôle des voyageurs aux frontières¹³⁹⁵.

La lutte contre la fraude documentaire est devenue une priorité pour les dirigeants européens, surtout après les attentats qui ont touché la France en 2015, la Commission ayant constaté que près de 5000 Européens avaient rejoint les rangs des combattants de l'État islamique¹³⁹⁶. Avant même les attentats du Bataclan et de Charlie Hebdo, les ministres européens avaient rendu des conclusions encourageant l'utilisation des « frontières intelligentes » et des bases de données nationales et européennes. Les attentats de Paris de novembre 2015 avaient montré que Daesh disposait de 200 000 faux documents d'identité. Les attentats du Bataclan et de Charlie Hebdo ont non seulement mis en lumière la gravité de la menace, mais les attaques de novembre 2015 à Paris ont également révélé l'importance cruciale des déplacements transfrontaliers dans la lutte contre le terrorisme. De son côté, le coordinateur européen pour la lutte antiterroriste constatait, dans un rapport de mars 2016, que ce type de fraude est

¹³⁹³ D. THOMSON, *Les Revenants, Ils étaient partis faire le jihad, ils sont de retour en France*, Éditions Seuil, 2016.

¹³⁹⁴ C. PUDLOWSKI, « David Thomson : "L'Europe est condamnée à subir le contre-choc des erreurs qui ont été faites" », *Slate*, 20 décembre 2016, en ligne à URL : <https://www.slate.fr/story/131831/erreurs-medias-dijihadisme> consulté le 17 mai 2023.

¹³⁹⁵ P. BERTHELET, « La sécurité digitale à l'heure des crises migratoire et terroriste, le nœud gordien de l'interconnexion des fichiers », *GDR ELSJ*, 20 avril 2016, en ligne à URL : <http://www.gdr-elsj.eu/2016/04/20/cooperation-judiciaire-penale/la-securite-digitale-a-lheure-des-crises-migratoire-et-terroriste-le-noeud-gordien-de-linterconnexion-des-fichiers/#more-4794> consulté le 17 mai 2023.

¹³⁹⁶ European Commission, op. cit.

préoccupant, surtout pour les détenteurs de faux documents qui souhaitent s'introduire dans l'espace européen pour commettre des attentats¹³⁹⁷.

Pour repérer les faux passeports et identifier leurs porteurs, différents moyens ont été mis en œuvre comme les contrôles opérés par du personnel de l'agence Europol, le déploiement d'agents spécialisés dans les zones sensibles grecques et italiennes avec le soutien des experts en documents, ALDO, de Frontex chargé de contribuer aux procédures d'identification en collaboration avec les équipes de filtrage nationales et le recours aux bases de données européennes. Les autorités publiques procèdent ainsi à diverses vérifications des migrants au regard d'une série de bases existantes dont les fichiers nationaux de police, le SIS II, le VIS, Eurodac, le Système d'information Europol, Prüm et le FADO (Faux documents et documents authentiques en ligne) qui est une base de données de fichiers européens recensant les documents de voyage et d'identité¹³⁹⁸.

Les progrès techniques permettent aujourd'hui aux services répressifs d'identifier des personnes recherchées à partir de données relatives aux étrangers déclarés indésirables et de générer des alertes à partir de l'usage d'images biométriques du visage, dit morphing. Les avancées en matière d'intelligence artificielle, dite *deep learning*, augmentent les possibilités offertes par l'usage des systèmes d'information.

Néanmoins, l'interconnexion des différents systèmes d'information n'est pas sans poser des problèmes de protection de la vie privée, même si la directive PNR, qui a vu s'affronter partisans et adversaires d'une sécurité numérique accrue, a été approuvée par le Parlement européen le 14 avril 2016, tout comme la directive sur la protection des données dans le secteur de la police et de la justice, également approuvée par lui le même jour. Nul doute que l'interopérabilité des systèmes d'information, nœud gordien d'une lutte contre le terrorisme et la criminalité internationale mêlée aux questions migratoires, donne toujours lieu à d'âpres débats sur le terrain des droits fondamentaux.

De l'autre côté, la sophistication des moyens de commettre des crimes, notamment les infractions terroristes, se développent à une vitesse accrue. Cette criminalité est nourrie par un contexte international dans lequel les conflits à travers le monde perdurent, accompagnés de crises climatiques et migratoires qui menacent chaque pays avec un débordement des frontières. Ces frontières sont aujourd'hui aux centres des débats et la notion de Nation ainsi que d'identité nationale sont plus que jamais d'actualité. L'intrusion des acteurs privés et la

¹³⁹⁷ P. BERTHELET, op. cit.

¹³⁹⁸ Ibidem

privatisation des aéroports viennent introduire des concepts qui rendent la compréhension de la réalité juridique de l'utilisation des données des passagers aériens encore plus complexe.

La surveillance des frontières est ainsi devenue un exemple où la privatisation des aéroports et la participation d'acteurs privés créent un appel d'air pour les grands groupes privés qui espèrent proposer des réponses aux nouvelles menaces globales en même temps que les gouvernements européens exigent des standards de protection très élevés aux frontières, notamment dans les aéroports, afin de renforcer la sécurité intérieure et éviter les attaques terroristes contre les aéroports européens comme ce fut le cas pour celui de Bruxelles. D'ailleurs, depuis cette attaque terroriste, tous les passagers doivent dorénavant présenter « une preuve de voyage (document électronique ou itinéraire) à la tente-marquise de l'entrée pour être admis à la salle de préenregistrement (aire d'attente avant les comptoirs d'enregistrement) »¹³⁹⁹.

La lutte contre le crime organisé et la prévention contre les activités transfrontalières illégales terrestres requièrent la mise en œuvre de systèmes de surveillance et de contrôle complets et précis avec des solutions comme la surveillance efficace des frontières, la détection jusqu'à interception, l'adaptation à la diversité des menaces terroristes et l'optimisation du déploiement et de l'utilisation des différentes ressources techniques et humaines. L'utilisation des données personnelles des passagers devient un élément pilier dans la conception de solutions de surveillance des frontières, dans les aéroports notamment, pour identifier les menaces terroristes, recenser les tactiques utilisées pour franchir les frontières d'un pays et suivre le type d'individus susceptibles de commettre des infractions terroristes¹⁴⁰⁰.

Le traitement « intelligent » des données à caractère personnel, en automatisant la détection et l'évaluation des menaces, aspire à mieux cibler les interventions dans les aéroports¹⁴⁰¹. Toutefois, dans une zone privatisée et hautement sensible, aucune recherche ne semble aujourd'hui expliquer l'anticipation et la neutralisation des menaces terroristes soient possibles, grâce à l'utilisation des données personnelles des passagers aériens, est possible sans la mise en danger du droit à la protection des données à caractère personnel et à la vie privée. Pour les États, il y a certes le probable bénéfice de frontières bien contrôlées, avec un haut niveau de protection des passagers, mais il n'est pas certain que la protection des

¹³⁹⁹ Air Transat, « Aéroport de Bruxelles : Nouvelles mesures de sécurité », en ligne à URL : <https://www.airtransat.com/fr-CA/nouvelles/archives/aeroport-de-bruxelles-avis-de-voyage> consulté le 8 juin 2023.

¹⁴⁰⁰ Thales, « La surveillance des frontières, un défi complexe », Surveillance des frontières, en ligne à URL : <https://www.thalesgroup.com/fr/global/activities/security/state/surveillance-des-frontieres> consulté le 8 juin 2023.

¹⁴⁰¹ Ibidem

données des passagers aériens soit encore possible de manière effective dans un cadre juridique incomplet de ce point de vue, car il ne prend pas en compte ce phénomène de privatisation des aéroports.

Si la privatisation des aéroports n'est pas encore hégémonique dans le monde, la participation des acteurs privés à la sûreté aéroportuaire est en hausse significative. Des entreprises comme Thales et Inetum ont ainsi unis leurs compétences pour fournir leur expertise en matière de sécurité et de commodité aux aéroports de Valence et Bilbao, tout en projetant d'en faire de même pour l'aéroport de Fuerteventura¹⁴⁰². L'installation d'accès « intelligents » fait partie des solutions proposées pour améliorer le passage aux frontières grâce à un processus de contrôle précis et rapide visant ainsi à faciliter de manière effective les opérations des agents de la police nationale.

Ces opérateurs privés, spécialisés dans la sécurité numérique, ont ainsi équipés les aéroports de Valence et de Bilbao de plus de 45 portes automatiques de contrôle¹⁴⁰³, de type ABC Gates, en s'appuyant sur la reconnaissance et la vérification automatique des documents. Le système ABC est un système d'identification et de vérification des documents qui permet d'identifier le passager au moyen d'une double vérification biométrique, image faciale et empreinte digitale¹⁴⁰⁴. Dans les deux aéroports espagnols, Thales a pour mission de veiller à la vérification d'identité et du contrôle d'accès intelligent et Inetum celle de mettre en œuvre les systèmes de surveillance en temps réel et les vérificateurs manuels¹⁴⁰⁵. Ces nouvelles technologies sont censées améliorer les performances en augmentant la sécurité, la souplesse et la commodité lors des contrôles d'identité biométriques dans les bases de données de police. Cette technologie n'enlève pas de compétences aux agents des frontières qui conservent ainsi le contrôle complet des opérations et peuvent donc procéder à des contrôles de sécurité supplémentaires si cela semble nécessaire.

Aspirant à alléger l'expérience des passagers aux frontières, ces technologies traitent les données personnelles des passagers aériens en vérifiant l'identité du voyageur et ses

¹⁴⁰² Thales, « Thales et Inetum améliorent le passage aux frontières dans les aéroports espagnols de Valence et Bilbao », 25 mars 2021, en ligne à URL : <https://www.thalesgroup.com/fr/group/journaliste/press-release/thales-et-inetum-ameliorent-le-passage-aux-frontieres-aeroports> consulté le 8 juin 2023.

¹⁴⁰³ Ibidem

¹⁴⁰⁴ Digital Security Magazine, « Le système ABC est mis à jour pour accélérer les citoyens à franchir les frontières dans les aéroports », 5 octobre 2012, en ligne à URL : <https://www.digitalsecuritymagazine.com/fr/2012/10/05/el-sistema-abc-system-se-actualiza-para-agilizar-a-los-ciudadanos-el-cruce-de-fronteras-en-aeropuertos/> consulté le 8 juin 2023.

¹⁴⁰⁵ CNIL, « Reconnaissance faciale dans les aéroports : quels enjeux et quels grands principes à respecter ? », 9 octobre 2020, en ligne à URL : <https://www.cnil.fr/fr/reconnaissance-faciale-dans-les-aeroports-quels-enjeux-et-quels-grands-principes-respecter> consulté le 8 juin 2023.

documents de voyage, notamment à travers les contrôles biométriques qui sont effectués. La reconnaissance faciale, comme les autres techniques, ne sont pas sans enjeux pour les droits fondamentaux des citoyens, la CNIL ayant rappelé que l'utilisation de la reconnaissance faciale pour le contrôle de l'identité dans les aéroports a des conséquences non-négligeables pour les droits et les libertés des personnes concernées.

Par conséquent, la CNIL recommandait d'intégrer de fortes garanties en matière de protection de données à caractère personnel. Les défis de l'introduction de la reconnaissance faciale dans les aéroports est vu avec sérieux puisqu'elle est assimilée à un traitement de données particulièrement sensibles, qui doit donc faire l'objet d'une protection renforcée. Pour la CNIL, cette nouvelle technologie discutée appartient « à la catégorie plus large des techniques biométriques qui permettent de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, physiologiques ou comportementales »¹⁴⁰⁶.

Dès lors qu'elles permettent ou visent l'identification unique d'une personne, ces caractéristiques sont qualifiées de « données biométriques » ; elles sont également qualifiées par la CNIL de données « sensibles » au sens du droit européen. Elles suivent un régime juridique spécifique puisqu'en principe leur traitement est interdit et ne peut être mis en œuvre sauf dans certains cas énumérés par le règlement européen sur la protection des données à caractère personnel.

Cette technologie « sans contact » est assimilée à un acte intrusif qui inquiète les autorités puisqu'elle a cette particularité d'être produite par le corps de l'individu et le marque de façon définitive, car ses données sont uniques et permanentes dans le temps ; ainsi, le passager ne peut s'en affranchir. Elle accompagne de plus en plus l'utilisateur des aéroports dans ce parcours fait de multiples contrôles biométriques dématérialisés. Il existe ainsi un risque que cette technologie alimente un « sentiment d'accoutumance », fragilisant les droits et les libertés des citoyens¹⁴⁰⁷.

Pour la CNIL, les grands principes du droit européen doivent être respectés, à savoir que le traitement des données des passagers doit être proportionné en termes d'impact pour les droits et les libertés des personnes, vis-à-vis de l'objectif ou de la finalité qu'il poursuit, et ne doit porter que sur des données « nécessaires » pour l'atteindre. C'est le cas pour le recours à un dispositif de reconnaissance faciale qui permet de fluidifier l'embarquement des passagers et

¹⁴⁰⁶ Ibidem

¹⁴⁰⁷ Ibid.

d'éviter la formation de files d'attente pour des motifs d'ordre sécuritaire. Il est proportionné selon les cas¹⁴⁰⁸.

Cette technique doit reposer sur le recueil préalable du consentement des passagers, conformément à l'article 9.2.a du RGPD qui requiert, pour que ce consentement soit valable, qu'il soit « libre, spécifique et éclairé ». Des mesures organisationnelles et techniques doivent être mises en œuvre afin de garantir que le dispositif de reconnaissance faciale traite uniquement les données de personnes ayant préalablement consenti : en installant une configuration technique floutant le visage des passagers se trouvant en arrière-plan ; en activant des caméras de reconnaissance faciale uniquement après une action du passager concerné ; en affichant des panneaux et des marquages au sol distinguant les zones de contrôle par reconnaissance faciale des zones de contrôle classiques.

Pour le cas des données biométriques, la CNIL insiste sur le besoin de privilégier la conservation desdites données sur un support dont l'autorité concernée a l'usage et le contrôle exclusif afin de limiter le risque de piratage lié à la centralisation de gabarits biométriques dans une base de données. En pratique, soit elle est stockée dans une base de données sous une forme chiffrée, la rendant inutilisable sans la communication, soit elle est stockée sur un support individuel dont le passager a la maîtrise et l'usage exclusif.

Enfin, la CNIL recommande la réalisation d'une analyse d'impact relative à la protection des données (AIPD) avant la mise en œuvre du traitement, qu'il soit expérimental ou non puisqu'il est ici question de données sensibles, d'un nombre important de passagers potentiellement concernés et de risques inhérents associés à ce type de passagers.

Souvent poussés par la volonté et la nécessité de s'adapter à une concurrence engagée et de réduire les dettes de l'État, les privatisations dépassent les enjeux du droit des sociétés ; elles portent des défis en termes politiques, sociaux, économiques et de libertés fondamentales. C'est naturellement le cas pour les aéroports puisqu'il est question ici d'un secteur vital et sensible, du point de vue de la sécurité du pays et de ses citoyens. Avec le développement croissant du secteur des transports aériens émerge un maillage d'aéroports nourri par l'essor constant de hubs mondiaux comme ceux de Dubaï ou d'Istanbul. Certains États ont gardé la propriété exclusive des aéroports tandis que d'autres ont cédé aux sirènes du libéralisme. Les débats sur le projet de privatisation des Aéroports de Paris s'inscrivent dans ce contexte bien que l'État français ne puisse se permettre de se dessaisir définitivement des actifs de la société du fait du principe de continuité du service public aéroportuaire. La crise du Covid-19 est

¹⁴⁰⁸ Ibid.

venue mettre un terme à ce débat et suspendre le projet de privatisation. Toujours est-il que les tenants du projet n'ont pas précisé de quelle manière ils allaient veiller à la protection des droits des voyageurs, notamment leur droit à la protection de la vie privée et leur droit à la protection des données personnelles, car la privatisation allait de fait, comme de droit, modifier l'économie de l'entreprise.

D'ailleurs, en 2018, la Cour des comptes a rendu un rapport¹⁴⁰⁹ critique vis-à-vis de l'ouverture du capital des sociétés aéroportuaires de Nice, de Toulouse et Lyon bien qu'elle se soit réalisée dans un contexte de forte croissance du trafic aérien, avec des degrés de valorisation supérieurs aux prévisions de l'État actionnaire. En effet, le processus de privatisation de l'aéroport de Toulouse a montré de sérieuses insuffisances et demeure inachevé mais il a été amélioré pour Nice et Lyon. De façon générale, les procédures de cession prennent peu en compte la dimension environnementale, industrielle et sociale des projets. L'État est appelé à se doter d'une stratégie globale, à définir précisément les intérêts qu'il entend protéger et à garder « un haut niveau d'information sur les décisions affectant la qualité du service public aéronautique »¹⁴¹⁰. Ces recommandations ont été indirectement rappelées lorsque la privatisation, aujourd'hui avortée, d'Aéroports de Paris avait été discutée.

Ce transfert des actifs publics à des acteurs privés est au point mort aujourd'hui et les difficultés persistent encore pour concilier les volontés autour du mouvement de privatisation et le maintien des impératifs liés au maintien du service public aéroportuaire. Les privatisations n'ont pas remis en cause le système de concession de service public, ni n'ont affecté le transfert de biens publics aéroportuaires à des acteurs privés, mais elles n'ont pas fourni l'assurance que les passagers garderaient un accès à des prix de voyages abordables et seraient protéger efficacement dans leurs droits fondamentaux, y compris le droit à la vie privée et le droit à la protection des données à caractère personnel, face à l'intrusion de nouveaux acteurs non étatiques, souvent motivés par une volonté non-avouée d'utiliser ces données en tant que valeur ajoutée économique au détriment de leur garantie.

¹⁴⁰⁹ Cour des comptes, « Le processus de privatisation des aéroports de Toulouse, Lyon et Nice », Communication à la commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale, octobre 2018, en ligne à URL <https://www.ccomptes.fr/system/files/2018-11/20181113-processus-privatisation-aeroports-Toulouse-Lyon-Nice.pdf> consulté le 8 mai 2023.

¹⁴¹⁰ X. DELPECH, « Un rapport critique sur les privatisations d'aéroports », *Dalloz*, Juris tourisme, Transport aérien, JT 2018, n° 214, p.7.

TITRE 2 – L’AFFAIBLISSEMENT DE LA PROTECTION JURIDIQUE DES DOSSIERS PASSAGERS PAR LA DÉTERRITORIALISATION

« Dans un livre comme dans toute chose, il y a des lignes d'articulation ou de segmentarité, des strates, des territorialités; mais aussi des lignes de fuite, des mouvements de déterritorialisation et de déstratification. Les vitesses comparées d'écoulement d'après ces lignes entraînent des phénomènes de retard relatif, de viscosité, ou au contraire de précipitation et de rupture. Tout cela, les lignes et les vitesses mesurables, constitue un agencement »¹⁴¹¹. Dans cet extrait de *Mille Plateaux*, Gilles Deleuze et Félix Guattari reprennent le concept de déterritorialisation qu'ils ont introduit pour la première fois en 1972 dans l'ouvrage *Anti-Œdipe*¹⁴¹². Cette attaque en règle contre la psychanalyse freudienne reproche au fameux neurologue autrichien d'avoir reterritorisé la libido sur le terrain du drame œdipien après avoir libéré le psychisme au moyen du concept de libido par le processus de déterritorialisation. Dans *Mille Plateaux*, les deux chercheurs français associent le concept de déterritorialisation au « corps-sans-organes », puis introduisent la distinction entre « déterritorialisation relative » et « déterritorialisation absolue ». C'est la première déclinaison qui va laisser place à une « reterritorialisation ».

Ce terme a ensuite été réutilisé dans d'autres branches des sciences humaines, par exemple en géographie humaine, puis a été transformé par cette réappropriation. D'une certaine façon, on pourrait dire que la notion elle-même a été « déterritorisée ». Repris par la littérature de la géographie culturelle, le concept désigne aujourd'hui le fait de rompre le lien de territorialité entre une société et un territoire. Ainsi, la déportation des Acadiens, désignée comme le « Grand Dérangement », est un exemple de déterritorialisation mais également lorsque les Anglais ont chassé, au milieu du XVIII^e siècle, des colons français de l'Amérique du Nord, du fait de leur refus de prêter allégeance à la Couronne britannique¹⁴¹³. Cette idée de rupture entre un territoire et des individus, ici désigné comme un groupe, peut également décrire le processus de dissociation, de rupture ou de décontextualisation. Dans le cadre des relations entre l'individu et les données de son dossier passager, la déterritorialisation représente une

¹⁴¹¹ G. DELEUZE, F. GUATTARI, *Mille plateaux*, Minuit, 1980.

¹⁴¹² G. DELEUZE, F. GUATTARI, *L'Anti-Œdipe*, Minuit, 1972.

¹⁴¹³ F. GLAIN, « Les immigrants acadiens au XVIII^e siècle, une colonie en Poitou », Centre Châtelleraudais d'Histoire et d'Archives, 2018, en ligne à URL : <http://ccha.fr/wp-content/uploads/2018/02/6-Acadiens-PDF.pdf> consulté le 12 juin 2023.

menace, car les données personnelles du passager circulent dans le monde à chaque vol aérien effectué, sans qu'il y ait nécessairement un contrôle complet sur ces dernières.

Il n'est alors pas surprenant de voir que le chercheur Fred Poché adapte le concept aux problématiques contemporaines, en évoquant « l'émergence d'un présent saturé, [qui] renvoie à la déterritorialisation continue que permet le numérique »¹⁴¹⁴. La déterritorialisation numérique modifierait ainsi la difficulté des individus de se rapporter au monde et créerait, selon le chercheur, un « malaise contemporain ». Cette lecture des bouleversements survenus avec l'émergence de l'espace « numérique » est faite dans une perspective sociologique, qui reproche la perte d'attention et « une focalisation sur la communauté d'élection ou d'origine, au détriment de la communauté de destin ».

Cette déterritorialisation numérique pourrait aussi désigner l'étoilement des données à caractère personnel des utilisateurs des transports aériens, qui fragilise la capacité des citoyens, notamment européens, à protéger de manière effective leurs droits fondamentaux, dont la protection des données à caractère personnel et de la vie privée. En effet, techniquement cette protection devient impossible du fait de la dispersion de ces données dans des espaces juridiques et techniques que leur droit d'origine est incapable d'appréhender et de sanctionner.

Le lien entre ces données à caractère personnel et le droit auquel elles se rattachent est distendu par l'absence d'un territoire commun sur lequel peut s'exercer concrètement et effectivement la réalité juridique européenne, censée protéger le droit à la protection des données à caractère personnel. En effet, les dossiers passagers aériens, suivant ces derniers à travers leurs voyages dans des centaines de destination à travers le monde, sont traités par des fors dont certains d'entre eux ne reconnaissent même pas le droit à la protection des données personnelles des passagers aériens.

Aujourd'hui, le territoire national est débordé par les mouvements de capitaux, de personnes et d'objets. La déterritorialisation peut être identifiée comme l'effacement de l'État territorial devant les flux supranationaux et transfrontaliers, causant l'affaiblissement des contrôles d'accessibilité, des frontières internationales, donc des contraintes spatiales imposées par l'État¹⁴¹⁵ (chapitre 1). Ces transformations ont pour conséquence un affaiblissement de la

¹⁴¹⁴ F. POCHÉ, « Diagnostiquer le mécontentement », *Revue Projet*, 29 janvier 2020, en ligne à URL : <https://www.revue-projet.com/articles/2020-01-poché-diagnostiquer-le-mecontentement/10464> consulté le 12 juin 2023.

¹⁴¹⁵ J.-M. PONTIER, « Territorialisation et déterritorialisation de l'action publique », *Actualité juridique*, Droit administratif, 1997.

protection juridique des données à caractère personnel puisque les droits nationaux et communautaires sont dépassés, incapables de régir des flux supranationaux. L'État est aujourd'hui concurrencé par divers acteurs qui tissent des flux internationaux, immatériels et matériels, qui modifient le sens des frontières.

Phénomène dans lequel les échanges économiques se déploient au-delà des frontières des États et selon une logique qui leur échappe, la mondialisation est venue interroger le sens des frontières dans les espaces étatiques contemporains, même chez ceux qui bénéficient d'une stabilité politique depuis plusieurs décennies. C'est le cas en Europe où la question de la souveraineté, du lieu de décision et du territoire est soulevée dans les débats publics. En effet, les actions qui visent à assurer la sécurité des citoyens, comme l'instauration des dossiers passagers, se discutent de moins en moins entre deux États-nations. C'est moins la fin des territoires que leur relativité qui est mise en avant par les dossiers passagers ; le territoire national devient de moins en moins une référence indiscutable autour duquel peut s'articuler toutes les politiques¹⁴¹⁶.

À cette crise des frontières s'ajoute celle du multilatéralisme avec un acteur important de la scène des relations internationales, et des dossiers passagers, à savoir les États-Unis d'Amérique qui sont tentés par l'unilatéralisme et l'isolement et refusent toujours d'adhérer à des instruments internationaux comme la Cour pénale internationale et les Accords de Kyoto.

L'État est parfois défié par des menaces venant de l'intérieur qui refusent le fait du prince et des forces exogènes¹⁴¹⁷ qui se déterritorialisent aussi, c'est le cas de groupes terroristes, comme Al-Qaïda¹⁴¹⁸ par exemple, que les dossiers passagers visent dans leur combat contre les infractions terroristes.

Pour la protection juridique des dossiers passagers, c'est une sérieuse menace qui se profile. Elle touche le territoire considéré comme un substrat de la localisation des activités humaines. Le territoire est une idée centrale dans toute organisation humaine, où l'individu, plus tard le citoyen, cherche à se fixer afin d'assurer son existence et la perpétuation du groupe auquel il appartient. Élément constitutif de l'État, le territoire est considéré comme une condition

¹⁴¹⁶ B. BADIE, *La Fin des territoires*, Fayard, 1995.

¹⁴¹⁷ Le Monde, « États-Unis : le chef d'extrême droite Stewart Rhodes condamné à dix-huit ans de prison pour "sédition" » lors de l'assaut du Capitole », 25 mai 2023, en ligne à URL : https://www.lemonde.fr/international/article/2023/05/25/etats-unis-le-chef-d-extreme-droite-stewart-rhodes-condamne-a-dix-huit-ans-de-prison-pour-sedition-lors-de-l-assaut-du-capitole_6174865_3210.html consulté en ligne le 13 juin 2023.

¹⁴¹⁸ J. CHICHIZOLA, « Vingt ans après, les fantômes d'al-Qaïda hantent toujours l'antiterrorisme français », *Le Monde*, 25 mai 2023, en ligne à URL : <https://www.lefigaro.fr/actualite-france/vingt-ans-apres-les-fantomes-d-al-qaïda-hantent-toujours-l-antiterrorisme-francais-20230522> consulté en ligne le 13 juin 2023.

déterminante de son existence. Les États-nations se définissent ainsi par l'existence de leur territoire rappelle Bertrand Badie¹⁴¹⁹.

Avec l'utilisation croissante des nouvelles technologies et la globalisation des échanges, le nombre de transferts de données hors de France n'a cessé de croître. Le transfert de données à caractère personnel hors de l'Union européenne et de l'Espace économique européen est courant. Toutefois, le droit européen est venu ajouter une condition à ce mouvement : assurer un niveau de protection de ces données approprié et suffisant. Ces transferts doivent obligatoirement être encadrés à travers différents outils juridiques. Les débats autour du transfert hors de l'Union européenne des données des citoyens européens révèlent également les craintes de ces derniers que les services de renseignement américains les espionnent de façon illégale¹⁴²⁰.

Par ailleurs, cette déterritorialisation peut être limitée par l'implication des États dans les crises contemporaines, ce fut le cas lors de la crise du Covid-19. Les États ont toujours joué toujours un rôle central dans ce type de crises. Leur souveraineté territoriale, leur politique étrangère, leur contrôle des frontières et leur diplomatie peuvent devenir des éléments qui limitent la déterritorialisation dans de nombreuses situations. Conséquemment, avec ces crises, les États restent des acteurs clés dans la gestion des crises. Le législateur national peut alors intervenir dans l'utilisation des données personnelles (chapitre 2).

¹⁴¹⁹ B. BADIE, *La fin des territoires*, Fayard, 1995

¹⁴²⁰ F. BAJAK, K. CHAN, « Biden order promises EU citizens better data privacy », *AP NEWS*, 7 octobre 2022, en ligne à URL : <https://apnews.com/article/biden-technology-data-privacy-ursula-von-der-leyen-european-commission-493ea47a4991b0c933bea2bbb47c2c6c> consulté en ligne le 14 juin 2023.

Chapitre 1 – Une déterritorialisation par le caractère supranational des dossiers passagers : l’effacement du droit national dans les transferts de données personnelles

Avec un développement incessant et croissant, le numérique crée d’immenses opportunités industrielles et économiques tout en soulevant d’importants enjeux démocratiques et géopolitiques. Face à la volonté de domination de divers acteurs étrangers, l’Union européenne développe son propre modèle en matière numérique, en cherchant un équilibre entre innovation et régulation, afin de traiter l’économie des plateformes, les contenus en ligne et la circulation des données, notamment à l’extérieur de l’Union.

Si la construction européenne a réussi à engendrer un marché commun, notamment celui du charbon, de l’acier, des produits agricoles, des marchandises, des services et des capitaux, celui du numérique voit encore se pointer des obstacles devant lui. Cette construction subit deux types de fragmentation. La première est une fragmentation causée par les disparités sociales, économiques et d’infrastructures entre États membres qui ne les placent pas sur un pied d’égalité, notamment en matière de digitalisation des administrations et des entreprises et sur le plan de l’accès du public aux outils numériques¹⁴²¹. Cette inégalité est aussi géographique, entre les pays du nord de l’Europe, performants dans ce domaine, ceux de l’ouest qui sont moyennement performants et enfin, ceux du sud et de l’est qui accusent du retard.

La seconde fragmentation est d’ordre législatif : chaque État membre semble appliquer pour l’essentiel ses propres règles à destination du secteur, en faisant fi des frontières ou, au contraire, en exploite ces disparités à son avantage. C’est le cas dans le domaine du géo-blocage, une technique qui proscriit ou limite l’accès des internautes à des contenus, sites ou services proposés dans un autre État membre. L’Union a interdit en 2018 cette discrimination pour les abonnements audiovisuels payants et le commerce en ligne¹⁴²². Ces spécificités du secteur numérique compliquent l’harmonisation du marché intérieur européen.

¹⁴²¹ L. LICTEVOUT, B. GAILLARD, « La politique numérique de l’Union européenne », *Toute l’Europe*, 27 mars 2023, en ligne à URL : <https://www.touteleurope.eu/economie-et-social/la-politique-numerique-de-l-union-europeenne/> consulté en ligne le 14 juin 2023.

¹⁴²² Règlement (UE) 2018/302 du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d’autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d’établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n° 2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE, article 1.

Ces dernières années, l'Union a ainsi aspiré à harmoniser les législations nationales tout en réglementant les activités du secteur à travers son propre modèle de régulation. En 1995, une directive a été adoptée sur la protection des données personnelles¹⁴²³. En 2018, le fameux RGPD a renforcé le principe de transparence des plateformes du numérique vis-à-vis de leur usage des informations à caractère personnel, a introduit un droit à la portabilité permettant aux utilisateurs de transférer ou récupérer ces données, et consacré un droit à l'oubli. Considéré actuellement comme une référence dans ce domaine, cette législation s'applique aussi bien aux sociétés européennes qu'aux acteurs étrangers proposant leurs services aux citoyens européens. Ce texte marque la volonté du législateur de surmonter les questions de fragmentation et de faire face au problème de la porosité des frontières contemporaines.

Le 26 janvier 2022, la Commission a présenté une « déclaration interinstitutionnelle solennelle » sur les principes et les droits numériques dans le cadre sa « décennie numérique ». Venant en complément des droits existants, notamment ceux ancrés dans la Charte des droits fondamentaux de l'Union et dans la législation en matière de protection des données et de vie privée, ces principes et droits ont pour objet de fournir un cadre de référence aux citoyens européens vis-à-vis de leurs droits numériques. L'un des droits cités est le renforcement de la sûreté, la sécurité et l'autonomisation des personnes¹⁴²⁴. Ce projet montre la volonté européenne de donner à ses citoyens les moyens d'agir dans un avenir numérique durable, centré sur l'humain et plus prospère. Au regard du traitement des données personnelles des passagers aériens, elle confirme la tendance de certaines institutions européennes, notamment la Cour de justice, d'essayer de trouver un équilibre entre la sécurité collective des Européens et la protection des droits fondamentaux dont ceux de la protection de la vie privée et des données à caractère personnel dans une séquence temporelle où les défis qui se posent aux États doivent être traités de façon de plus en plus complexe, car les crises qui se succèdent sont multiples et impliquent aussi bien la sécurité que l'écologie, l'économie et le social.

Pour les données à caractère personnel des passagers aériens, le caractère supranational des dossiers passagers implique une déterritorialisation qui a pour conséquence l'effacement du droit national en matière de transfert de ces derniers d'un espace à un autre (section 1). C'est le cas des accords signés entre les États-Unis d'Amérique et l'Union européenne sachant que

¹⁴²³ Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

¹⁴²⁴ Commission européenne, « Décennie numérique de l'Europe: objectifs numériques pour 2030 », 2022, en ligne à URL : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr consulté le 15 juin 2023.

les standards juridiques de chacun en termes de protection des données à caractère personnel sont clairement différents, les Européens étant plus impliqués dans la protection effective des droits fondamentaux de leurs citoyens en la matière tandis que les Américains qui considèrent l'utilisation des données comme un droit des entreprises¹⁴²⁵. Le stockage des dossiers passagers souffre aussi d'une fragile limitation temporelle (section 2).

Certains États membres jouent un rôle d'initiateur et d'appui politique non négligeable. C'est le cas de la France¹⁴²⁶, par exemple, qui a soutenu le projet de directive européenne avec sérieux, le voyant comme un outil nécessaire face au niveau extrêmement élevé de la menace terroriste. La directive était ainsi perçue et présentée comme « une étape indispensable dans le renforcement de la lutte contre le terrorisme en Europe »¹⁴²⁷. Les États membres jouent ainsi un rôle dans la mise en place des législations qui encadrent le transfert des données personnelles des passagers aériens sachant que la tendance générale est l'effacement de leurs législations face à des accords à caractère supranational.

Section 1 – Le transfert des dossiers passagers : l'extension de l'extraterritorialité au détriment d'un espace protecteur des droits des passagers

Avec la mondialisation des échanges et l'utilisation continue des nouvelles technologies, le nombre de transferts de données hors de France ne cesse d'augmenter. Toutefois, les transferts de données en dehors de l'Union européenne et de l'Espace économique européen ne sont possibles en principe, nous l'avons vu, seulement si un niveau de protection des données adéquat et approprié est assuré. Ces transferts sont appelés à être encadrés à l'aide de divers outils juridiques. Le cadre juridique européen, notamment le RGPD, énonce que les responsables de traitement et les sous-traitants peuvent transférer des données à caractère personnel de l'espace européen, à la condition de garantir un niveau de protection des données approprié et suffisant. À cet égard, la jurisprudence des juges de Luxembourg a eu un impact sur le cadre juridique européen relatif au transfert des données personnelles en sanctionnant les accords qui ne protégeaient pas suffisamment les droits fondamentaux des citoyens européens.

¹⁴²⁵ S. A. WARREN, « Staying on top of data privacy », *India Business Law Journal*, *Ikigai Law*, 22 mars 2023, en ligne à URL : <https://law.asia/data-protection-laws> consulté le 15 juin 2023.

¹⁴²⁶ Gouvernement français, « Adoption du PNR européen : une étape indispensable dans le renforcement de la lutte contre le terrorisme », *Argumentaire*, 15 avril 2016, en ligne à URL : <https://www.gouvernement.fr/argumentaire/adoption-du-pnr-europeen-une-etape-indispensable-dans-le-renforcement-de-la-lutte-4405> consulté le 15 juin 2023.

¹⁴²⁷ Ibidem

Le 16 juillet 2020, la CJUE a ainsi rendu un arrêt majeur, dit « Schrems II »¹⁴²⁸, invalidant le régime de transferts de données entre l'Union européenne et les États-Unis, dénommé *Privacy shield*. Cet arrêt a eu de nombreuses conséquences pour les entités qui souhaitaient transférer des données outre-Atlantique. Globalement, les juges européens considéraient la législation américaine comme étant non-compatible avec les standards européens. Cette législation étrangère, qui s'applique aux données transférées, conduit à fragiliser les protections que fournissent ces instruments et nécessitent ainsi, selon les juges européens, la mise en place de mesures supplémentaires. L'arrêt a par ailleurs invalidé la décision d'adéquation de la Commission européenne à l'égard des États-Unis : son analyse de la législation américaine, notamment s'agissant du système de surveillance américain, l'a amenée à considérer que les atteintes portées au droit à la vie privée des individus dont les données sont traitées par les opérateurs et les entreprises états-uniens soumis au droit américain sont disproportionnées au regard des principes de la Charte des droits fondamentaux européenne¹⁴²⁹.

En réponse à cette invalidation en juillet 2020 du *Privacy Shield* par la CJUE, le président américain Joe Biden a adopté un nouveau cadre juridique, en édictant un *Executive Order* le 7 octobre 2022¹⁴³⁰ visant à renforcer les garanties américaines en matière de collecte et d'utilisation de données personnelles par les services de renseignement. Ce nouveau cadre juridique a été soumis à la Commission européenne afin qu'elle évalue s'il assure une protection adéquate des données européennes. La Commission a soumis, le 13 décembre 2020, un projet de décision au CEPD, l'instance qui regroupe toutes les autorités européennes de protection des données, pour avis avant qu'elle décide d'adopter une décision reconnaissant l'adéquation de ce nouvel instrument juridique. Le 28 février 2023, le CEPD a rendu son avis sur l'adéquation sur le projet de décision de la Commission européenne qui, tout en constatant les améliorations apportées par le nouveau cadre juridique américain, a fait savoir que des inquiétudes subsistaient sur un certain nombre de points dont il a dressé la liste¹⁴³¹.

¹⁴²⁸ CJUE, arrêt du 16 juillet 2020, Schrems II, affaire C-311/18. Voir en ce sens : CNIL, « Présentation de l'arrêt de la CJUE », 23 juin 2021, en ligne à URL : <https://www.cnil.fr/fr/presentation-de-larret-de-la-cjue> consulté le 30 juin 2023.

¹⁴²⁹ Ibidem

¹⁴³⁰ Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, 7 octobre 2022. Voir en ce sens : CNIL, « Transfert de données vers les États-Unis : le CEPD rend son avis sur le projet de décision d'adéquation de la Commission européenne », 23 mars 2023, en ligne à URL : <https://www.cnil.fr/fr/transfert-de-donnees-vers-les-etats-unis-le-cepd-rend-son-avis-sur-le-projet-de-decision-dadequation> consulté le 30 juin 2023

¹⁴³¹ CEPD, avis 5/2023 relatif au projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE-États-Unis, 28 février 2023.

Pour les données des passagers aériens, la directive PNR 2016/681 du 27 avril 2016 est venue réglementer l'utilisation des données des dossiers passagers faisant ainsi figure de droit spécial par rapport au RGPD. Recueillies par les transporteurs aériens, ces données sont transmises aux autorités sécuritaires des États membres aux fins de prévention et de détection d'infractions terroristes et de crimes graves. La directive PNR a pour objet de réglementer le transfert des données passagers par les compagnies aériennes aux autorités nationales. Après la collecte de ces données, les autorités répressives peuvent confronter les données à caractère personnel des passagers aériens à diverses bases de données de personnes disponibles.

La directive PNR encadre le traitement systématique des données des passagers pour les vols hors espace européen, à destination et en provenance de l'Union européenne, ainsi que pour les vols à l'intérieur de l'espace européen, si les États membres le prévoient. Ces données ne peuvent être utilisées qu'à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité, d'enquête et de poursuites. Ces finalités constituent donc une exception à l'application matérielle du RGPD dont l'article 2.d) exclut de son champ d'application le traitement de données par les autorités compétentes « à des fins de prévention et de détection des infractions pénales (...) y compris la protection contre des menaces pour la sécurité publique »¹⁴³².

Les juges de Luxembourg ont ainsi distingué l'application du RGPD et de la directive PNR au regard du traitement des données à caractère personnel des passagers aériens. En effet, concernant le recueil et le transfert des données de passagers aériens par les transporteurs aériens aux unités d'information des passagers, le RGPD est applicable tandis que la directive PNR est applicable pour le seul « traitement de données » par l'UIP ou par les autorités nationales, aux fins de lutte contre le terrorisme¹⁴³³.

Avec cette directive, les Européens ont d'abord fait face de manière réaliste à l'extraterritorialité du droit américain, qui oblige les compagnies aériennes à transmettre les données des passagers aériens souhaitant atterrir en Europe. Ensuite, cet acte juridique européen prenait en compte les activités liées au terrorisme et à la criminalité organisée, facilitées par la fluidité des déplacements internationaux des individus (sous-section 1). Enfin, le droit européen, comme les accords internationaux, ont mis en avant leur volonté

¹⁴³² G. HAAS, « Directive PNR : la CJUE recadre le traitement des données de passagers aériens », *HAAS Avocats*, le Blog, 16 août 2022, en ligne à URL : <https://info.haas-avocats.com/droit-digital/directive-pnr-la-cjue-recadre-le-traitement-des-donnees-de-passagers-aeriens#:~:text=La%20directive%20PNR%20vise%20C3%A0,de%20donn%C3%A9es%20de%20personnes%20recherch%C3%A9es>, consulté le 30 juin 2023.

¹⁴³³ CJUE, 21 juin 2022, n° C-817/19, *Ligue des droits humains c/ Conseil des ministres*.

d'harmoniser les législations en matière de dossiers passagers pour éviter l'insécurité juridique et les failles en matière sécuritaire, sans pour autant démontrer la garantie effective du droit à la protection des dossiers passagers¹⁴³⁴, en particulier dans les cas de transferts transfrontaliers (sous-section 2).

Sous-section 1 – La multiplication des actes juridiques privilégiant la fluidité des transferts transnationaux des données à caractère personnel

Des accords bilatéraux aux directives et règlements européens en passant par divers mécanismes juridiques, plusieurs actes juridiques permettent le transfert transnational des données à caractère personnel. Ces flux de données transférées ont parfois été remis en cause lorsque les droits fondamentaux des citoyens européens n'ont pas été effectivement garantis.

§ 1 – Une législation européenne d'encadrement des transferts de données à caractère personnel vers les pays tiers en construction

Un principe existe dans le droit européen depuis plusieurs années ; celui de l'interdiction du transfert de données à caractère personnel si le pays destinataire n'est pas capable d'assurer un niveau de protection suffisant de ces données¹⁴³⁵. Les États membres ont donc pour obligation de prévoir, dans leur législation nationale, l'interdiction du transfert de données personnelles vers tout pays tiers à l'Union européenne qui ne garantit pas le niveau de protection exigé. En France, l'article 226-16 du Code pénal sanctionne jusqu'à cinq ans d'emprisonnement et 300 000 euros d'amende le non-respect des formalités préalables de déclaration ou autorisation¹⁴³⁶. L'article 226-22-1 du même code prévoit que « le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés [...] est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende »¹⁴³⁷.

¹⁴³⁴ Consilium Europa, « Directive de l'UE relative aux données des dossiers passagers (PNR) », *Action de l'UE face au terrorisme*, Conseil européen – Conseil de l'Union européenne, 31 août 2022, en ligne à URL : <https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/passenger-name-record/#:~:text=La%20directive%20PNR%20r%C3%A9glemente%20le,des%20poursuites%20en%20la%20mat%C3%A8re>, consulté le 30 juin 2023.

¹⁴³⁵ CNIL, « Les transferts de données à caractère personnel hors Union européenne », en ligne à URL : <https://www.cnil.fr/fr/transférer-des-donnees-hors-de-lue#:~:text=Le%20cadre%20g%C3%A9n%C3%A9ral%20pr%C3%A9vu%20par,des%20donn%C3%A9es%20suffisant%20et%20appropri%C3%A9>, consulté le 3 juillet 2023.

¹⁴³⁶ Code pénal, article 226-16.

¹⁴³⁷ Code pénal, article 226-22-1.

Ce principe est repris dans le RGPD qui précise qu' « un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si [...] les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis »¹⁴³⁸. Cet encadrement strict était devenu nécessaire avec l'utilisation croissante des nouvelles technologies dans un contexte de globalisation des échanges, rendant le nombre de transferts de données hors d'Europe de plus en plus important. Fixer des conditions s'avérait donc nécessaires si les États membres souhaitaient garder un niveau de protection des données approprié et suffisant. Si le niveau de protection qu'offre le pays de destination n'est pas adéquat, alors le transfert hors de l'Union européenne desdites données ne peut être effectué qu'en présence de certaines garanties appropriées ou à des conditions très strictes selon le RGPD. Les transferts de données avec les États-Unis illustrent les difficultés auxquelles les autorités européennes peuvent être confrontées lorsqu'elles mènent des discussions avec des pays extérieurs à l'UE. Le règlement 2016/679 a considérablement élargi son champ d'application territorial, sous réserve que les conditions de transfert ne changent pas de nature. Contrairement à l'approche européenne, les États-Unis ont tendance à adopter la voie contractuelle et l'auto-régulation en matière de protection des données personnelles, n'ayant dans leur arsenal juridique que quelques législations sectorielles. Par conséquent, à moins de bénéficier de l'une des exceptions prévues par le droit européen, la transmission de données personnelles vers les entités américaines est en principe interdite¹⁴³⁹.

Selon la CNIL, « on parle de transfert de données à caractère personnel lorsque ces données sont transférées depuis le territoire européen vers un ou des pays qui n'appliquent pas les dispositions de la directive 95/46(1) (il s'agit des pays ni membres de l'Union européenne, ni membres de l'Espace économique européen). Le transfert peut s'effectuer par communication, copie ou déplacement de données, par l'intermédiaire d'un réseau (par ex. : accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de

¹⁴³⁸ RGPD, article 44.

¹⁴³⁹ C. FERAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », in *Praxis Cyberdroit*, LexisNexis, chapitre 115, 2021.

support (par ex. : d'un disque dur d'ordinateur à un serveur) »¹⁴⁴⁰. Cette interprétation inclut des opérations telles que la centralisation intragroupe de la base de données liées aux ressources humaines impliquant le transfert de données du personnel, la centralisation intragroupe de la base de données de gestion des commandes et de la comptabilité clients ou un transfert vers un client aux fins de saisie informatique de dossier manuel¹⁴⁴¹.

Des limites ont été posées par la jurisprudence, c'est le cas avec l'arrêt Lindqvist¹⁴⁴² de la CJUE rendu le 6 novembre 2003 dans lequel les juges européens ont considéré que l'inscription de données personnelles relatives à des individus sur une page internet ne constituait pas un transfert de données vers un pays tiers. Elle rendait ainsi ces informations accessibles à des individus dans ces pays tiers. De même, le fait qu'une personne communique activement des informations la concernant à une entité située dans un pays tiers ne suffit pas à caractériser un tel transfert¹⁴⁴³.

Un transfert de données personnelles vers un pays tiers ou une organisation internationale est autorisé si la Commission constate, par voie de décision, que ledit pays, un territoire de celui-ci ou un secteur lui appartenant, ou bien l'organisation en question, assurent un niveau de protection adéquat. Ces transferts ne nécessitent pas d'autorisation spécifique¹⁴⁴⁴.

Il appartient à la Commission de décider quels pays offrent un niveau de protection adéquat sur la base des exigences européennes. En effet, celle-ci se prononce sur certains éléments : la protection des libertés fondamentales, la législation, l'accès aux données personnelles par les autorités publiques, l'existence et le fonctionnement de régulateurs indépendants, l'engagement du pays de destination. Une fois qu'une décision d'adéquation a été prise, aucune autorisation spécifique n'est requise pour les transferts hors de l'espace européen. Toutefois, cette décision est amenée à être révisée au moins tous les quatre ans¹⁴⁴⁵. La décision de constat d'adéquation peut être abrogée, modifiée ou suspendue dans le cas où la Commission constate que le niveau de protection est inadéquat. La Commission publie au Journal officiel de l'Union européenne (JOUE) et sur son site internet une liste des pays tiers, des territoires et

¹⁴⁴⁰ CNIL, « Les transferts de données à caractère personnel hors Union européenne », en ligne à URL : <https://www.cnil.fr/fr/transférer-des-données-hors-de-lue#:~:text=Le%20cadre%20g%C3%A9n%C3%A9ral%20pr%C3%A9vu%20par,des%20donn%C3%A9es%20suffisant%20et%20appropri%C3%A9>. consulté le 3 juillet 2023

¹⁴⁴¹ C. FERAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », in *Praxis Cyberdroit*, LexisNexis, chapitre 115, 2021.

¹⁴⁴² CJUE, arrêt du 6 novembre 2003, Lindqvist, affaire C-101/01.

¹⁴⁴³ CJUE, 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein GmbH, affaire C-210/16.

¹⁴⁴⁴ C. FERAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », in *Praxis Cyberdroit*, LexisNexis, chapitre 115, 2021.

¹⁴⁴⁵ Ibidem

des secteurs spécifiques ainsi que des organisations internationales qu'elle juge, par voie de décision, ayant réalisé la condition d'adéquation ou non¹⁴⁴⁶. Ainsi, la Suisse et l'Argentine ont bénéficié d'une décision d'adéquation tandis que le Canada et les États-Unis bénéficient d'une décision d'adéquation partielle car le premier est reconnu adéquat seulement pour les transferts réalisés dans le secteur commercial relevant de la législation canadienne PIPEDA sur la protection des renseignements personnels et les documents à caractère électroniques et, s'agissant du second, il ne bénéficie de la couverture d'adéquation que pour les entreprises qui se sont engagées à respecter les règles européennes.

En l'absence de décisions d'adéquation, le responsable de traitement ou le sous-traitant ne peut permettre le transfert de données à caractère personnel vers un pays tiers ou une organisation internationale qu'à la condition qu'ils soient prévues des garanties appropriées et que les personnes concernées disposent de voies de droit effectives et de droits opposables¹⁴⁴⁷. Lesdites garanties peuvent être octroyées sans qu'une autorisation particulière de l'autorité de contrôle ne soit requise par un instrument juridiquement contraignant et exécutoire entre les organismes et autorités publiques, par des règles d'entreprises contraignantes, par des clauses contractuelles type de protection adoptées par la Commission européenne ou par une autorité de contrôle et approuvées par la Commission, par un code de conduite ou encore un mécanisme de certification approuvés¹⁴⁴⁸.

En l'absence d'une décision d'adéquation ou de garanties appropriées, un transfert hors de l'Union européenne ne peut se réaliser que si l'une des conditions suivantes est remplie : la personne concernée a donné son consentement, le transfert est nécessaire à l'exécution d'un contrat ou à la mise en œuvre de mesures précontractuelles ; le transfert est nécessaire pour des motifs importants d'intérêt public, à la constatation, à l'exercice ou à la défense de droits en justice ; le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ; le transfert a lieu au départ d'un registre destiné à fournir des informations au public et est ouvert à la consultation du public ou à toute personne justifiant d'un intérêt

¹⁴⁴⁶ 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.

¹⁴⁴⁷ Ibidem.

¹⁴⁴⁸ RGPD, article 46.

légitime sous certaines limites ; le transfert est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable de traitement¹⁴⁴⁹.

§ 2 – L'échec de la Commission dans la mise en place d'un mécanisme de transfert des données personnelles de l'Union européenne vers les États-Unis

Les autorités américaines privilégient généralement les approches contractuelles et l'autorégulation pour la protection des données personnelles, complétées par quelques lois sectorielles spécifiques. À l'opposé, l'approche européenne se caractérise par une architecture juridique complète et une législation globale dans ce domaine¹⁴⁵⁰.

Historiquement, sur le fondement de l'article 25-5 de la directive européenne 95/46, aujourd'hui abrogée, des négociations avaient été engagées dès 1996 entre la Commission et le Département du commerce américain. En octobre 1998, à l'occasion de la conférence d'Ottawa sur le commerce électronique, les participants ont considéré qu'un niveau de protection adéquat demande au minimum l'adoption de règles nées des lignes directrices de l'Organisation de coopération et de développement économiques (ci-après OCDE) de 1980¹⁴⁵¹. Ce travail a poussé le gouvernement américain à mettre sur la table de nouvelles versions des principes *Safe Harbor* qui n'ont toutefois pas su convaincre le G29. Ce dernier, dans un avis 7/99 du 3 décembre 1999, a considéré que le niveau de protection proposé par le Gouvernement américain restait en dessous de celui requis par l'Union européenne¹⁴⁵².

Après de longues négociations entre les États membres sur les *Safe Harbor principles*, la Commission a rendu une décision le 26 juillet 2000 dans laquelle elle considérait que les sociétés américaines avaient publiquement et volontairement adhéré à ces règles présumées assurer un niveau de protection adéquat. Selon le dispositif adopté, les entreprises adhérentes devaient décrire leurs activités, leurs propres règles de protection de la vie privée et des données à caractère personnel, ou déclarer adhérer à un dispositif de non-divulgaration et désigner un organisme indépendant à saisir en cas de plainte à leur encontre. Elles devaient aussi notifier au département américain du commerce leur engagement à adhérer à des principes de nature très similaire à la directive 95/46. Les entreprises qui n'étaient pas

¹⁴⁴⁹ 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) n° 45/2001 et la décision n° 1247/2002/CE (Texte présentant de l'intérêt pour l'EEE.)

¹⁴⁵⁰ G. BESNIER, « Le règlement général sur la protection des données personnelles », *Le Taurillon*, 28 mai 2018.

¹⁴⁵¹ J.DRYDEN, « Un monde sans frontières : concrétiser le potentiel du commerce électronique mondiale », *L'Observateur de l'OCDE*, 1999.

¹⁴⁵² G29, avis 7/99 du 3 décembre 1999. Voir en ce sens : C. FERAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », *Praxis Cyberdroit*, LexisNexis, chapitre 115, 2021.

membres de la sphère de sécurité et celles qui n'en bénéficiaient pas ne pouvaient généralement pas profiter des dérogations prévues par l'article 26 de la directive 95/46.

Quelques années plus tard, le scandale des écoutes par les agences américaines a conduit les institutions américaines à reconsidérer leurs politiques concernant les flux de données entre Européens et Américains. Il mettra fin au mécanisme *Safe Harbor*.

Tout a commencé le 6 juin 2013 lorsque le journal britannique *The Guardian* a révélé que l'opérateur téléphonique Verizon et d'autres opérateurs américains livraient chaque jour à la National Security Agency (NSA, « l'Agence nationale de la sécurité »), à la demande du Federal Bureau of Investigation (FBI), la totalité des données téléphoniques en leur possession concernant les communications téléphoniques sur le sol américain, mais aussi entre les États-Unis et les États étrangers¹⁴⁵³. Une ordonnance de justice, qui n'a pas été rendue publique, forçait l'opérateur à fournir ces informations. Elle était renouvelée tous les trois mois, depuis au moins sept ans, comme le précisa la présidente de la commission du renseignement du Sénat américain¹⁴⁵⁴.

Ce même jour, *The Guardian* et *The Washington Post* ont en outre révélé le programme de surveillance PRISM qui permettait au FBI et à la NSA d'espionner les internautes du monde entier. L'opération était rendue possible par l'utilisation des passerelles cachées dans les logiciels produits par les grandes sociétés informatiques américaines et permettait un accès via les serveurs de neuf d'entre elles, dont Microsoft, Yahoo, Google, Facebook et Apple. Parmi les informations volées figurait une présentation PowerPoint, généralement destinée aux employés de la NSA, sur le fonctionnement du programme PRISM¹⁴⁵⁵. Le 7 juin 2013, le journal *The Guardian* révéla le contenu d'une directive présidentielle top secrète signée par Barack Obama en octobre de la même année. La directive détaillait l'approche américaine des

¹⁴⁵³ T. BERTHEMET, « Edward Snowden, l'homme qui fait trembler le gouvernement américain », *Le Figaro*, 10 juin 2013, en ligne à URL : <https://www.lefigaro.fr/international/2013/06/10/01003-20130610ARTFIG00394-etats-unis-edward-snowden-un-whistleblower-contre-la-nsa.php> consulté le 6 juillet 2023.

¹⁴⁵⁴ G. GREENWALD, « Anger swells after NSA phone records court order revelations », *The Guardian*, 6 juin 2013, en ligne à URL : <https://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records> consulté le 6 juillet 2023.

¹⁴⁵⁵ B. GELLMAN, L. POITRAS, « U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program », *The Washington Post*, 6 juin 2013, en ligne à URL : https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1 consulté le 6 juillet 2023.

cyberopérations offensives et demandait aux responsables de la sécurité nationale d'élaborer une liste de cibles potentielles pour les cyberattaques¹⁴⁵⁶.

D'autres révélations ont continué de créer de l'embarras au sein des chancelleries occidentales comme celle qui faisait état de l'espionnage des bureaux de l'Union, en pénétrant leurs réseaux informations, par les services de renseignements américains¹⁴⁵⁷. Ces révélations ont endommagé les relations entre l'Union et les États-Unis d'un point de vue politique¹⁴⁵⁸. Elles ont ensuite entraîné des conséquences sur un plan juridique.

Le Parlement européen a réagi avec vigueur en adoptant un rapport sur la surveillance de masse réalisée par les États-Unis le 12 mars 2014 concluant à la nécessité de la suspension immédiate de l'accord *Safe Harbor*¹⁴⁵⁹. Quelques mois plus tard, un arrêt de la CJUE du 6 octobre 2015¹⁴⁶⁰ a annulé la décision du 26 juillet 2000¹⁴⁶¹, ayant mis en place le mécanisme *Safe Harbor* qui avait consacré le principe de libre transfert des données personnelles depuis l'Union européenne vers les États-Unis.

En l'espèce, le ressortissant autrichien M. Maximilian Schrems, utilisateur de Facebook, a contesté devant l'autorité irlandaise de protection des données à caractère personnel (Data Protection Commissionner irlandais) le transfert de ses données par une filiale irlandaise de Facebook vers des serveurs situés aux États-Unis. Le requérant estimait que la législation et la pratique américaines n'offraient pas une protection adéquate aux données personnelles stockées aux États-Unis, car elles étaient accessibles à la NSA et à d'autres agences de sécurité américaines lors de campagnes de surveillance et d'interception à grande échelle et non ciblées. Son appel a été rejeté, les autorités irlandaises ont conclu que les États-Unis assuraient une protection adéquate des données personnelles et que Facebook était en conformité avec le mécanisme *Safe Harbor*.

¹⁴⁵⁶ B. FERRAN, « Prism : Apple, Microsoft et Facebook se confessent timidement » [archive], *Le Figaro*, 17 juin 2013, en ligne à URL : <https://www.lefigaro.fr/secteur/high-tech/2013/06/17/32001-20130617ARTFIG00582-prism-apple-microsoft-et-facebook-se-confessent-timidement.php> consulté le 6 juillet 2023.

¹⁴⁵⁷ N. VERSIEUX, « Berlin et Bruxelles tirent les grandes oreilles de l'Amérique », *Libération*, 30 juin 2013.

¹⁴⁵⁸ Le Monde.fr avec AFP et Reuters, « Prism : la NSA espionnait l'Union européenne », *Le Monde*, 29 juin 2013, en ligne à URL : https://www.lemonde.fr/ameriques/article/2013/06/29/prism-la-nsa-espionnait-l-union-europeenne_3439112_3222.html consulté le 6 juillet 2023.

¹⁴⁵⁹ C. FERAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », in *Praxis Cyberdroit*, LexisNexis, chapitre 115, 2021.

¹⁴⁶⁰ CJUE, 6 octobre 2015, Maximilian Schrems c/ Digital Rights Ireland Ltd, affaire C-362/14, R. N ; CCE 2015, n° 11, comm. 94, note A. Debet.

¹⁴⁶¹ Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique.

Puis, la High Court of England a été saisie. Celle-ci a soumis à l'appréciation de la CJUE une question préjudicielle visant à déterminer si l'autorité nationale était soumise à la décision de la Commission européenne du 26 juillet 2000 qui autorise le transfert de données à caractère personnel depuis le sol américain vers les entreprises enregistrées aux États-Unis qui se sont engagées à respecter les règles du mécanisme *Safe Harbor* ou si elle pouvait faire sa propre enquête, notamment sur la base de faits postérieurs.

En ce qui concerne les pouvoirs de l'autorité de contrôle, la Cour a estimé que la décision de la Commission ne pouvait ni les supprimer ni les réduire. Elle a fait valoir que même si une telle décision est prise, ces autorités doivent pouvoir examiner en toute indépendance si les transferts de données vers des pays tiers sont conformes aux exigences de la directive 95/46. La Cour a jugé, nonobstant une décision contraire de la Commission, qu'une demande de contestation du niveau de protection adéquat dans un pays tiers doit être comprise comme impliquant la compatibilité d'une telle décision avec la protection des droits fondamentaux des personnes concernées, conformément à la directive 95/46 et à la Charte des droits fondamentaux de l'Union.

S'agissant de la validité de la décision du 26 juillet 2000, la Cour a considéré que la notion de niveau de protection adéquat doit s'entendre comme imposant aux États tiers d'assurer effectivement un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti par l'Union¹⁴⁶². En l'espèce, le juge européen a considéré qu'aux États-Unis, les principes *Safe Harbor* auxquels adhéraient les entreprises assuraient la protection des données personnelles alors que les autorités gouvernementales n'étaient pas liées par ces principes. La Cour releva que ces règles pouvaient être écartées si elles entraient en conflit avec la sécurité nationale, l'intérêt public ou les exigences de la loi américaine, en constituant une ingérence dans les droits fondamentaux. Or, la décision mise en cause ne faisait aucune mention de règles visant à limiter ces ingérences.

Après l'invalidation du système *Safe Harbor*, le transfert de données vers les États-Unis requerrait, d'une part, la mise en place de *Binding Corporate Rules* (BCR) ou la conclusion de clauses contractuelles types pour pouvoir continuer à garantir le transfert de données personnelles dans des conditions conformes au droit européen et, d'autre part, le consentement des individus dont les données à caractère personnel sont transférées vers le sol américain.

¹⁴⁶² CJUE, Maximillian Schrems c/ Data Protection Commissioner, affaire C-362/14, 6 octobre 2015.

§ 3 – Le droit européen face à la position antagoniste du droit américain en matière de transfert des données à caractère personnel

En invalidant le mécanisme *Safe Harbor* le 6 octobre 2015¹⁴⁶³, la Cour de justice a conduit les gouvernements européens et les institutions de l'Union européenne à engager de nouvelles discussions avec le Gouvernement américain. Ces négociations donneront lieu à l'accord *Privacy Shield* qui remplaça le 12 juillet 2016 le mécanisme *Safe Harbor*. Ce nouveau dispositif prévoyait un « bouclier de protection des données UE-EU » auquel les sociétés américaines devaient adhérer ainsi qu'une « décision sur le caractère adéquat du niveau de protection » qui actaient les engagements pris par le Gouvernement des États-Unis dans la mise en œuvre du dispositif¹⁴⁶⁴. Précisément, le mécanisme a mis en place des obligations strictes pour les entreprises devant traiter ces données. Le nouveau régime prévoyait des mécanismes de contrôle efficaces pour s'assurer que les entreprises respectent leurs obligations, y compris des sanctions ou l'exclusion en cas de non-respect ; les conditions de transfert ultérieur à d'autres partenaires étaient également plus strictes.

Un mécanisme de médiation était aussi prévu dans le cadre dudit bouclier. Le Gouvernement américain, par l'intermédiaire des services du directeur du renseignement national, a fourni des assurances écrites aux autorités européennes selon lesquelles tout accès gouvernemental aux données à des fins de sécurité nationale sera soumis à des restrictions, des conditions et des mécanismes de surveillance clairs qui empêchent un accès généralisé aux données personnelles. Le secrétaire d'État américain s'était, de son côté, engagé à offrir aux citoyens de l'Union une possibilité de recours dans le domaine du renseignement national en établissant un mécanisme de médiation au sein du département d'État indépendant des services de sécurité nationale¹⁴⁶⁵. Le médiateur avait pour mission de garantir le suivi des demandes et des plaintes d'information des particuliers et leur notifiait si la législation pertinente avait été respectée. Ces engagements devaient être publiés au *Federal Register* américain¹⁴⁶⁶.

Il existait aussi un mécanisme de règlement extrajudiciaire des litiges. Les entreprises qui avaient adhéré au bouclier devaient apporter une réponse aux plaintes reçues dans les quarante-cinq jours. Ce mécanisme était accessible sans frais. Les citoyens européens pouvaient par ailleurs s'adresser à l'autorité compétente de leur pays en charge de la

¹⁴⁶³ CJUE, 6 octobre 2015, *Maximillian Schrems c/ Digital Rights Ireland Ltd*, affaire C-362/14, préc.

¹⁴⁶⁴ C. FERAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », in *Praxis Cyberdroit, LexisNexis*, chapitre 115, 2021.

¹⁴⁶⁵ *Ibidem*

¹⁴⁶⁶ T. MINSEN, C. SEITZ, M. ABOY, M. C. COMPAGNUCCI, « The EU-US Privacy Shield Regime for Cross- Border Transfers of Personal Data under the GDPR », *Lexion*, 2020.

protection des données à caractère personnel pour collaborer avec son homologue américain et s'assurer que les plaintes déposées par les personnes concernées, au sein de l'Union européenne, puissent être étudiées et traitées.

Un mécanisme d'arbitrage¹⁴⁶⁷ était également prévu dans le cas où le litige n'était pas réglé par l'un de ces moyens afin de trouver une solution qui puisse être applicable. De plus, les entreprises pouvaient s'engager à respecter les recommandations émises par les autorités européennes de protection des données. Les entreprises qui utilisent des données en lien avec les ressources humaines devaient également faire de même.

Un mécanisme de révision annuelle était également prévu afin de contrôler le fonctionnement du bouclier, notamment le respect des engagements et des garanties d'accès aux données à des fins d'ordre public et de sécurité nationale. L'examen était dirigé par la Commission européenne et le département américain du commerce et impliquait des experts nationaux du renseignement travaillant avec les agences américaines et européennes de protection des données. La Commission s'appuyait sur toutes les autres sources d'information disponibles, y compris les rapports de transparence publiés par les entreprises indiquant dans quelle mesure les autorités publiques ont demandé l'accès aux données¹⁴⁶⁸.

Le 18 octobre 2017, la Commission européenne a présenté son rapport sur le premier examen annuel des opérations du *Privacy Shield* dans lequel elle constata que les autorités américaines avaient mis en place les structures et procédures nécessaires pour garantir la protection des données personnelles¹⁴⁶⁹. Puis, elle formula dix recommandations visant à assurer le fonctionnement normal et continu du *Privacy Shield*, en encourageant le département américain du commerce à surveiller de manière proactive et régulière le respect par les entreprises de ses obligations qui prévoyaient que ces dernières ne devaient pas faire publiquement référence à leur certification de conformité au mécanisme tant que le processus de certification n'était pas terminé. Des recherches devaient ainsi être faites en cas de fausses déclarations. La Commission a également recommandé la nomination d'un médiateur pour traiter les plaintes des citoyens concernant l'ingérence des autorités américaines dans leurs droits et mener une campagne de sensibilisation auprès des citoyens européens.

¹⁴⁶⁷ M-A. WEISS, « De la sphère au bouclier : qu'est-ce que le Privacy Shield ? », *I2D - Information, données & documents*, 2016/3 (Volume 53), pp. 20-22, En ligne à URL : <https://www.cairn.info/revue-i2d-information-donnees-et-documents-2016-3-page-20.htm> consulté le 7 juillet 2023.

¹⁴⁶⁸ C. FERAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », in *Praxis Cyberdroit*, LexisNexis, chapitre 115, 2021.

¹⁴⁶⁹ Commission européenne, *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield*, {SWD(2017) 344 final}, 18 octobre 2017.

Cependant, le 16 juillet 2020, la CJUE a rendu un arrêt majeur, dit « Schrems II », qui a invalidé le régime *Privacy shield* de transferts de données entre l'Union européenne et les États-Unis¹⁴⁷⁰. En l'espèce, les juges européens ont d'abord consacré la validité des clauses contractuelles (CCT) tout en indiquant que pour en bénéficier, il appartient au responsable de traitement, le cas échéant en coopération avec le destinataire des données personnelles transférées, de juger si, en pratique et pour le transfert envisagé, ces clauses permettent de garantir aux données transférées un niveau de protection essentiellement équivalent à celui assuré au sein de l'Union européenne. Si l'effet de celles-ci est limité ou totalement mis de côté par la loi du pays tiers applicable aux transferts de ces données, le responsable de traitement doit appliquer des mesures additionnelles pour assurer le niveau de protection des données à caractère personnel requis ou notifier l'autorité compétente de sa volonté de continuer à transférer des données sans ces garanties.

La Cour a analysé la loi¹⁴⁷¹ américaine en matière d'accès aux données des fournisseurs de services Internet et entreprises de télécommunications par les services américains de renseignement. Les juges européens ont conclu que les atteintes portées à la vie privée des individus dont les données sont traitées par les entreprises et opérateurs américains soumis à cette loi sont disproportionnées au regard des principes de la Charte des droits fondamentaux. En particulier, la CJUE a considéré que la collecte des données à caractère personnel par les services de renseignement n'est pas proportionnée et que les voies de recours, y compris juridictionnelles, dont disposent les personnes vis-à-vis du traitement de leurs données sont insuffisantes. Conséquemment, la Cour a invalidé la décision d'adéquation de la Commission européenne¹⁴⁷².

Tous les transferts de données à caractère personnel vers les États-Unis sont liés par les conséquences de cette décision, car la législation en cause, la Section 702 FISA et l'Executive Order 12 333, couvre tous les fournisseurs de service internet et les entreprises de télécommunications basées aux États-Unis. Par conséquent, l'accès, par les services américains de renseignements, aux données traitées par ces opérateurs peut intervenir une fois les données transférées et stockées vers le sol américain mais également durant leur transit vers cet espace, bien que le destinataire des données ne soit pas lui-même concerné par la loi en cause.

¹⁴⁷⁰ CNIL, « Présentation de l'arrêt de la CJUE », 23 juin 2021, en ligne à URL : <https://www.cnil.fr/fr/presentation-de-larret-de-la-cjue> consulté le 9 juillet 2023.

¹⁴⁷¹ Section 702 FISA et Executive Order 12 333.

¹⁴⁷² CJUE, affaire C-311/18, 16 juillet 2020.

Cette décision a eu un impact sur tous les transferts de données à caractère personnel ; quelle que soit la nature de transfert et la qualité des entités concernées, quel que ce soit le responsable du traitement et le sous-traitant. Du fait de la globalisation, avec la multiplication des échanges et l'utilisation croissante des technologies, le nombre de flux de données transférées hors de France ne cesse d'augmenter. Cette jurisprudence confirme que le transfert de données hors de l'Union est possible mais les autorités compétentes doivent assurer d'un niveau de protection de données à caractère personnel approprié et suffisant. Les juges veulent ainsi encadrer ces transferts de manière sérieuse.

Après cet arrêt, la Commission a défini de nouvelles règles au titre du RGPD pour le transfert des données personnelles vers des pays tiers. Elle a ainsi demandé que les transferts frontaliers¹⁴⁷³ intègrent les nouvelles clauses contractuelles standards, fassent l'objet d'un examen au cas par cas pour déterminer si les données seront suffisamment protégées au regard des droits légaux. Lorsque la loi en vigueur du pays ne permet pas de protéger d'une manière équivalente à celle garantie dans l'espace européen, des mesures complémentaires aux clauses contractuelles types sont nécessaires pour amener le niveau de protection aux normes européennes. Le non-respect de ces exigences est rappelé par le RGPD qui prévoit une amende pouvant aller jusqu'à 4% du chiffre d'affaires mondial de l'entreprise concernée.

L'association qui œuvre pour une meilleure protection de la vie privée et de la protection des données personnelles, basées en Autriche et dont le fondateur est Max Schrems, None of Your Business (NOYB)¹⁴⁷⁴, a choisi au mois d'août 2020 d'opter pour une interprétation maximaliste de l'arrêt en considérant que le simple fait de travailler avec un opérateur américain était, en soi, contraire à l'arrêt de la Cour de justice. Dans ce contexte, l'entité autrichienne avait préparé une plainte à l'encontre de 101 entreprises basées en Europe et travaillant avec Facebook et Google. Le but de NOYB était de faire cesser toute relation d'affaires entre les entreprises américaines et européennes. L'arrêt a créé beaucoup d'incertitude dans le paysage européen, notamment parce que les entreprises n'ont pas disposé d'une période de transition pour s'adapter aux changements inhérents à cette invalidation.

¹⁴⁷³ CNIL, « Présentation de l'arrêt de la CJUE », 23 juin 2021, en ligne à URL : <https://www.cnil.fr/fr/presentation-de-larret-de-la-cjue> consulté le 9 juillet 2023

¹⁴⁷⁴ R. BOUCQ, « Schrems II : répercussion française », *Administratif IP/IT et Communication*, Dalloz, 21 octobre 2020, en ligne à URL : <https://www.dalloz-actualite.fr/node/schrems-ii-repercussion-francaise> consulté le 10 juillet 2023.

Sous-section 2 – L’encadrement juridique du transfert transfrontalier des données à caractère personnel des passagers aériens

Les données personnelles des passagers sont des informations fournies par ces derniers à l’agence de voyages ou à la compagnie aérienne lorsqu’ils procèdent à la réservation de leur vol. Utilisées par les services de sécurité, ces données servent à identifier les criminels dangereux et les terroristes. Elles ont ainsi permis aux autorités d’appréhender les terroristes responsables de la planification d’une attaque à la bombe dans le métro de New York en 2009¹⁴⁷⁵. Après les attaques terroristes en 2008, ces informations ont permis d’appréhender les responsables de l’attaque visant le Times Square en 2010¹⁴⁷⁶. Ces données constituent aussi un élément non négligeable pour identifier et lutter contre les trafiquants de drogue. Le transfert frontalier de ces données a fait l’objet de plusieurs textes dont le premier est l’accord de 2007 entre l’Union européenne et les États-Unis¹⁴⁷⁷.

§ 1 – Une volonté américaine imposant le transfert transfrontalier des données PNR objet de controverses

Avec la signature de l’accord entre Européens et Américains, les transporteurs aériens ont été obligés de réaliser des transferts de données de passagers vers les États-Unis et puis vers d’autres pays sans forcément savoir que ces destinataires garantissaient un niveau adéquat de protection de ces données¹⁴⁷⁸. Cette obligation découlait des lois américaines adoptées après les attentats du 11 septembre 2001 qui sont venues renforcer la sécurité du transport aérien américain et modifier de manière stricte les conditions d’entrée sur le sol américain, en contraignant sous peine d’amende, voire d’interdiction d’opérer, les transporteurs aériens à transférer aux agences américaines, préalablement au vol, les données personnelles des passagers en partance pour les États-Unis.

Christiane Féral-Schuhl rappelle l’avis du G29 qui a considéré que la transmission des données des passagers aériens entre pays, dans le cadre de la lutte contre le terrorisme et le

¹⁴⁷⁵ Europa, « Accord entre l’Union européenne et les États-Unis concernant les données des dossiers des passagers aériens », *Eux-Lex*, 26 août 2021, en ligne à URL : <https://eur-lex.europa.eu/FR/legal-content/summary/eu-us-agreement-on-airline-passenger-name-record-data.html#:~:text=les%20personnes%20auront%20le%20droit,quinze%20ans%20pour%20le%20terrorisme> consulté le 10 juillet 2023.

¹⁴⁷⁶ Ibidem

¹⁴⁷⁷ P. DE HERT & V. PAPAKONSTANTINO, “The PNR Agreement and Transatlantic Anti-terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic”, *Law, AARN: Topics of Concern in Applied Anthropology* (Topic), 1^{er} juin 2009, en ligne à URL : <https://www.semanticscholar.org/paper/The-PNR-Agreement-and-Transatlantic-Anti-terrorism-Hert-Papakonstantinou/c37bdfdd20026061e97bd8ed5b1e48dfca1d03c4> consulté le 10 juillet 2023.

¹⁴⁷⁸ C. FERAL-SCHUHL, « Des droits de la personne renforcés », *Les données personnelles*, Praxis Cyberdroit, Dalloz, 2020-2021.

crime organisé, a été critiquée¹⁴⁷⁹. Cette transmission déviait de l'objectif initial des données. En effet, celles-ci avaient été recueillies pour des motifs commerciaux, et non pour des raisons de sécurité. Malgré ces réserves, en mars 2003, avec l'accord de la Commission européenne, les autorités américaines ont obtenu un accès direct aux systèmes de réservation des principales compagnies aériennes desservant les États-Unis, soulevant des questions sur le respect des normes européennes en matière de protection des données.

Passé le 28 mai 2004, l'accord prévoyait que les données des passagers aériens transmises aux douanes et à la protection des frontières des États-Unis seront protégées de manière adéquate. Après audition des députés européens, la Cour a décidé le 30 mai 2006¹⁴⁸⁰ d'annuler l'accord de Washington du 28 mai 2004 au motif que les décisions d'adéquation prises par la Commission n'entraient pas dans le champ d'application de la directive européenne en vigueur à l'époque sur laquelle elle s'était basée. En effet, la directive 95/46 excluait le traitement des données « ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal ». Toutefois, le transfert de données des dossiers passagers constituait « un traitement ayant pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal ». Néanmoins, pour des raisons de sécurité juridique, la Cour a considéré que la décision d'adéquation de la Commission resterait en vigueur jusqu'au 30 septembre 2006¹⁴⁸¹.

Un nouvel accord entre les parties sur le transfert de ces données a été conclu le 23 juillet 2007 et est entré en vigueur le 1^{er} août 2007¹⁴⁸², fondé sur divers engagements pris par le ministère américain de la Sécurité intérieure et applicable à titre provisoire. Le 5 mai 2010, le Parlement européen a adopté une résolution demandant une renégociation de l'accord et le 2 décembre 2010¹⁴⁸³, le Conseil a autorisé la Commission à négocier un nouvel accord avec les autorités américaines sur les transferts de données des dossiers passagers. Paraphé le 17 novembre 2011, ce nouvel accord prévoyait le transfert de 19 catégories de données telles que le nom du passager, l'itinéraire de voyage et le lieu d'achat du billet, ainsi qu'un certain

¹⁴⁷⁹ Groupe 29, avis 4/2003 sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers. Voir : C. FÉRAL-SCHUHL, Données en matière pénale, *Dalloz*, *Praxis Cyberdroit*, Chapitre 134, 2021.

¹⁴⁸⁰ CJCE, 30 mai 2006, aff. C-317/04 et C-318/04, *Parlement européen c/ Conseil de l'Union européenne et Commission des Communautés européenne*, Rec. I-04721s; D. 2006. 1560.

¹⁴⁸¹ R. RIVAIS, « Le transfert de données passagers aux États-Unis jugé illégal », *Le Monde*, le 30 mai 2006.

¹⁴⁸² Conseil, décision n° 2007/551/PESC/JAI, 23 juillet 2007 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), JOUE L 204/16, 4 août 2007.

¹⁴⁸³ Parlement européen, résolution 5 mai 2010 sur le lancement des négociations sur les accords relatifs aux données des passagers aériens (PNR) avec les États-Unis, l'Australie et le Canada.

nombre de garanties en matière de protection des données à caractère personnel. L'accord a été conclu dans le cadre du troisième pilier qui regroupe les questions de police et de justice. Le ministère américain de l'Intérieur pouvait transférer les données des dossiers passagers à d'autres autorités gouvernementales. Ce ministère avait également accès, dans des circonstances exceptionnelles, aux données sensibles, c'est-à-dire celle pouvant révéler l'origine raciale et ethnique, les convictions religieuses, les opinions politiques et les données de santé. Aussi, les finalités du système sont très larges et évolutives¹⁴⁸⁴.

Dans son avis du 9 février 2012¹⁴⁸⁵, le CEPD a fait valoir deux remarques d'ordre général. D'une part, le contrôleur européen a rappelé que la Charte des droits fondamentaux de l'Union européenne estime que toute restriction des droits et des libertés doit être nécessaire, proportionnée et prévue par la loi. Or, en ce qui concerne l'accord euro-américain, la nécessité et la proportionnalité des systèmes PNR et des transferts de données vers les pays tiers n'avaient pas encore été prouvées. D'autre part, il a reconnu certaines améliorations par rapport à l'accord de 2007 et relevé l'existence de dispositifs de protection appropriés pour la sécurité et la supervision des données. Cependant, il a aussi souligné que les principales préoccupations exprimées dans les avis précédents et les conditions exigées par le Parlement européen n'avaient pas été respectées¹⁴⁸⁶. Ces deux remarques générales ont précédé des remarques relatives à d'autres manquements de l'accord vis-à-vis des droits fondamentaux et notamment de la protection des données personnelles prévus par le droit européen.

Bien que l'accord ait été accueilli favorablement, le CEPD a exprimé encore un certain nombre de préoccupations, notamment sur « les catégories de données à transférer au DHS »¹⁴⁸⁷. Les préoccupations du CEPD relèvent d'une approche globale européenne visant à concilier la sécurité collective et la liberté individuelle, que l'on retrouve aussi dans la résolution du Parlement du 5 mai 2010 indiquant que « les principes de nécessité et de proportionnalité sont essentiels pour mener une lutte efficace contre le terrorisme »¹⁴⁸⁸. Trouver le juste équilibre entre sécurité et liberté est un défi permanent pour les gouvernements du monde. En effet, assurer la sécurité de la collectivité sans violer les libertés

¹⁴⁸⁴ P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

¹⁴⁸⁵ Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure, 9 février 2012.

¹⁴⁸⁶ Ibidem

¹⁴⁸⁷ Ibid.

¹⁴⁸⁸ Résolution du Parlement européen du 5 mai 2010 sur le lancement des négociations sur les accords relatifs aux données des passagers aériens (PNR) avec les États-Unis, l'Australie et le Canada, 10 mai 2010.

des citoyens est l'une des missions que l'État doit remplir. Cette mission s'est accompagnée d'outils qui ont évolué dans le temps, selon les principes traditionnels d'alignement des services publics. Alors que les menaces à l'ordre public, et donc à la sécurité collective, se multiplient, l'arsenal judiciaire s'ajuste sous le contrôle du juge¹⁴⁸⁹.

L'article 49 U.S.C. § 44909 (c) (3) autorise la collecte des données des passagers aériens par les autorités américaines en charge du contrôle des frontières et l'article 19 CFR § 122.49d détaille les exigences essentielles du système PNR américain. Les données sont exigées de tout transporteur, qu'il soit américain ou non, pour les vols à destination ou au départ des États-Unis, y compris lorsque les passagers ont été contrôlés ou inspectés dans l'État de départ. Cet article définit les données PNR en des termes généraux : « Passenger Name Record (PNR) information refers to reservation information contained in an air carrier's electronic reservation system and/or departure control system that sets forth the identity and travel plans of each passenger or group of passengers included under the same reservation record with respect to any flight covered » (19 CFR § 122.49d, (b), (1))¹⁴⁹⁰.

Une même acception extensive s'applique vis-à-vis du contenu des données en question : « the air carrier, upon request, must provide Customs with electronic access to any and all PNR data elements relating to the identity and travel plans of a passenger concerning any flight under paragraph (a) of this section, to the extent that the carrier in fact possesses the requested data elements in its reservation system and/or departure control system »¹⁴⁹¹ (19 CFR § 122.49d, (b), (2)). La liste des informations susceptibles d'être requises correspond aux 19 catégories transférées dans les dossiers passagers sachant que les autorités américaines prennent en compte le fait que les compagnies aériennes ne sont parfois pas en possession de l'ensemble de celles-ci¹⁴⁹². Le transfert des données des passagers soulève de nombreuses préoccupations du point de vue de la protection des droits fondamentaux. En effet, sous l'influence du droit américain, les compagnies aériennes collectent ces données à des fins

¹⁴⁸⁹ F. CHALTIEL, « L'équilibre entre sécurité et liberté devant le juge constitutionnel », *Actu-juridique*, Droit constitutionnel, 11 juillet 2019, en ligne à URL : <https://www.actu-juridique.fr/constitutionnel/lequilibre-entre-securite-et-liberte-devant-le-juge-constitutionnel/> consulté le 10 juillet 2023.

¹⁴⁹⁰ Article 19 CFR § 122.49d. Traduction : « Les informations Passenger Name Record (PNR) font référence aux données de réservation contenues dans le système de réservation électronique et/ou le système de contrôle des départs d'une compagnie aérienne. Ces informations indiquent l'identité et les plans de voyage de chaque passager ou groupe de passagers associés au même enregistrement de réservation pour tout vol concerné ». Voir en ce sens : V. CORREA, « Fasc. 978 : Données des passagers aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

¹⁴⁹¹ Article 19 CFR § 122.49d, (b), (2). Traduction : « La compagnie aérienne, sur demande, doit fournir à la douane un accès électronique à tous les éléments de données PNR relatifs à l'identité et aux plans de voyage d'un passager concernant tout vol mentionné au paragraphe (a) de cette section, dans la mesure où la compagnie détient effectivement les éléments de données demandés dans son système de réservation et/ou son système de contrôle des départs ».

¹⁴⁹² Customs and Border Protection Passenger Name Record Privacy Policy, 21 juin 2013, p. 3.

sécuritaires. Or, il ressort des nombreux débats suscités par les accords sur les données PNR entre l'UE et les gouvernements des pays tiers que la possibilité de transferts de données entre autorités publiques est la question la plus préoccupante.

§ 2 – Des transferts de données PNR par les autorités publiques et les compagnies aériennes sujets d'inquiétudes

Avec l'initiative agressive et unilatérale du législateur américain, les compagnies aériennes qui collectaient les données personnelles des passagers aériens pour une utilisation exclusivement commerciale se voient désormais obligées de les transmettre aux agences publiques en charge de la sécurité des États de départ et/ou de destination de leurs vols.

A- Le transfert par les compagnies aériennes des données des passagers aériens, un encadrement en évolution

Le document 9944 de l'OACI énonce que les États n'ont pas le droit d'exiger les données des dossiers passagers détenues par une compagnie aérienne n'opérant pas physiquement un vol, mais qui a commercialisé le vol dans le cadre d'un accord de partage de code¹⁴⁹³. En effet, le standard « PNRGOV » est pensé afin que le transporteur aérien effectif, au lieu du transporteur ayant commercialisé le vol, soit le responsable de la transmission des données¹⁴⁹⁴. En contrepartie, le transporteur effectif doit fournir les données PNR des passagers qu'il transporte, sur la base d'un contrat de transport passé avec une autre compagnie aérienne. Ainsi, la directive PNR indique expressément que « lorsqu'il s'agit d'un vol en partage de code entre un ou plusieurs transporteurs aériens, l'obligation de transférer les données PNR de tous les passagers du vol incombe au transporteur aérien qui assure le vol »¹⁴⁹⁵.

Par ailleurs, lorsqu'un vol à destination ou au départ d'un État tiers comporte une ou plusieurs escales dans des aéroports des États membres de l'Union européenne, les transporteurs transfèrent les données des passagers aériens PNR de tous aux Unités information passagers (UIP) de tous les États membres concernés¹⁴⁹⁶.

Les exigences temporelles de transmission des données varient d'un État à un autre, une situation que déplorent de manière implicite l'OACI, l'IATA et la WCO. Toutefois, les règles

¹⁴⁹³ OACI, Guidelines on Passenger Name Record, préc., § 2.6.3

¹⁴⁹⁴ WCO/IATA/ICAO API Contact Committee, Principles, Functional and Business Requirements – PNRGOV, octobre 2013, p. 10

¹⁴⁹⁵ Directive (UE) 2016/681, 27 avril 2016, article 8 §1.

¹⁴⁹⁶ V. CORREA, « Fasc. 978 : Données des passagers aériens », LexisNexis, JurisClasseur Communication, 15 novembre 2019.

directrices relatives aux messages PNRGOV¹⁴⁹⁷ ont montré un certain consensus sur les approches de programmation d'envoi : toutes les données personnelles relatives à un vol précis sont envoyées « en bloc » et un nouveau fichier, par ailleurs complet, peut être envoyé plus tard pour faire état de modifications ou corrections ou tout simplement pour confirmation. L'article 8, paragraphe 3 de la directive PNR prévoit donc l'obligation de transférer les données 24 à 48 heures avant l'heure du décollage programmé du vol et une nouvelle fois immédiatement après la fermeture des portes de l'avion.

Toutefois, l'article 9¹⁴⁹⁸, paragraphe 4, de la même directive énonce que les États membres doivent autoriser les compagnies aériennes à limiter les transmissions, après la fermeture des vols, aux seules mises à jour des données. Les transporteurs aériens peuvent tout de même être amenés à transférer ces données à d'autres moments lorsque le demande une UIP¹⁴⁹⁹. Ces exigences sont reprises par le législateur français qui les a transposées à l'article R. 232-1-1, paragraphe I du Code de la sécurité intérieure. Dans ce contexte, la France a choisi d'autoriser que le second envoi soit limité aux seules mises à jour des données transférées lors du premier envoi. Aussi, l'article R. 232-1-1, paragraphe II du même code prévoit que « par dérogation, lorsque l'accès à des données de réservation et à des données d'enregistrement et d'embarquement est nécessaire pour répondre à une menace précise et réelle liée à une des infractions mentionnées au I de l'article L. 232-7, à l'exception des atteintes aux intérêts fondamentaux de la Nation, les transporteurs aériens transfèrent ces données, au cas par cas, en dehors des créneaux mentionnés au I du présent article, à la demande de l'Unité Information passagers, sur sollicitation des autorités mentionnées à l'article R. 232-15 »¹⁵⁰⁰.

Contrairement aux données API, les données des dossiers passagers ne sont pas transférées par les opérateurs aériens au moyen du standard « UN/EDIFACT "PAXLST" »¹⁵⁰¹ mais selon le format PNRGOV qui a été initialement développé par l'IATA¹⁵⁰². Ce dernier s'appuie sur des règles EDIFACT pour assurer un niveau acceptable d'interopérabilité, désormais dénommées les « PNRGOV EDIFACT ». Les principes directeurs relatifs aux messages

¹⁴⁹⁷ WCO/IATA/ICAO API Contact Committee, Principles, Functional and Business Requirements – PNRGOV, oct. 2013, p. 7.

¹⁴⁹⁸ Directive (UE) 2016/681, 27 avril 2016, préc., article 9, § 4.

¹⁴⁹⁹ Directive (UE) 2016/681, 27 avril 2016, préc., article 8, § 5.

¹⁵⁰⁰ Code de la sécurité intérieure, article 232-1-1.

¹⁵⁰¹ V. CORREA, « Fasc. 978 : Données des passagers aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

¹⁵⁰² IATA PADIS Standard v08.1.

PNRGOV¹⁵⁰³ soulignent la nécessité d'une acception harmonisée sur le plan international du dispositif pour une transmission automatisée effective des données¹⁵⁰⁴.

L'autorité nationale compétente accuse alors réception des données envoyées à travers le système utilisé par l'opérateur aérien au moyen d'un message appelé ACKRES - Acknowledge Receipt. Cela évite des difficultés relatives à la non-réception des données des dossiers passagers et prévient leur renvoi inutile. L'autorité nationale peut également envoyer par message GOVREQ (Government Request) une demande particulière relative à un vol ou un dossier PNR spécifique¹⁵⁰⁵.

Enfin, il convient de noter qu'un guide a été élaboré pour encadrer l'utilisation du format XML pour l'échange des messages PNRGOV¹⁵⁰⁶. En Europe, la décision européenne d'exécution 2017/759 de la Commission¹⁵⁰⁷ a contraint les opérateurs à utiliser les formats PNRGOV EDIFACT et le PNRGOV Formats XML. Par sa décision d'exécution, la Commission européenne¹⁵⁰⁸ impose l'utilisation du protocole IBM MQ ou du protocole IATA Type B, ou enfin ebMS 3.0 Versions 1.0 du profil AS4, une norme OASIS, publiées le 23 janvier 2013¹⁵⁰⁹.

B- Le transfert des données des passagers aériens entre autorités publiques, un encadrement controversé

a. Le transfert entre autorités nationales publiques, un cadre dominé par le principe du guichet unique

Selon l'Organisation mondiale des douanes (World Customs Organization, WCO), il est conseillé aux États de créer une « Unité de renseignements passagers » qui « jouera un rôle déterminant d'identification des voyageurs à haut risque sur la base des renseignements

¹⁵⁰³ WCO/IATA/ICAO API Contact Committee, Principles, Functional and Business Requirements – PNRGOV, octobre 2013.

¹⁵⁰⁴ WCO/IATA/ICAO API Contact Committee, EDIFACT Implementation Guide – PNR Data Pushed to States or Other Authorities – PNRGOV message, octobre 2013.

¹⁵⁰⁵ V. CORREA, « Fasc. 978 : Données des passagers aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

¹⁵⁰⁶ WCO/IATA/ICAO API Liaison Committee, XML Implementation Guidelines – PNR Data Pushing to States or Other Authorities – PNRGOV, octobre 2013.

¹⁵⁰⁷ Commission UE, décision d'exécution (UE) 2017/759 du 28 avril 2017 : JOUE n° L 113 du 29 avril 2017, p. 48

¹⁵⁰⁸ Commission EU, Implementing Decision (EU) 2017/759 du 28 avril 2017.

¹⁵⁰⁹ V. CORREA, « Fasc. 978 : Données des passagers aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

passagers fournis par les opérateurs aériens »¹⁵¹⁰. La directive européenne 2016/681 exige la désignation ou la création d'une autorité ayant pour compétence la prévention et la détection de menaces terroristes ou d'autres formes graves de criminalité.

Cette autorité, désignée « unité d'informations passagères » a pour mission de collecter, conserver et traiter les données de dossiers passagers. Elle est également responsable du transfert des données ou du transfert du résultat de leur traitement, aux autorités nationales compétentes (article 4, paragraphe 2, point a), ainsi qu'à l'UIP d'un autre État membre (article 4, paragraphe 2, point a) ou à Europol (article 4, paragraphe 2, b). Par ailleurs, l'article 4, paragraphe 4, de la directive autorise la création d'UIP conjointe, à deux États membres ou plus, bien que cela ne semble pas exister pour le moment¹⁵¹¹. Si les États membres choisissent de désigner une UIP commune, cette dernière sera considérée comme l'UIP de chaque État membre qui l'a créée.

L'unité d'information passagère française a été créée par le décret n°2014-1566 du 22 décembre 2014. Les décrets n° 2018-714 et 2018-722 du 3 août 2018, publié au Journal officiel du 8 août 2018, ont permis la transposition de la directive européenne 2016/681 et modifié ainsi le décret n° 2014-1566. L'unité française est conçue comme un service à compétence nationale placé sous l'autorité du ministre chargé des douanes. Ses missions, découlant des modifications introduites par l'article 1^{er}, § 2 du décret n° 2018-722, sont énoncées à l'article 2 du décret n° 2014-1566. Ainsi, cette unité doit collecter les données de réservation, d'enregistrement et d'embarquement des passagers du transport aérien ainsi que leur traitement, conservation ou transmission aux UIP d'autres États membres, aux autorités compétentes, ou à Europol¹⁵¹².

En France, l'UIP nationale est aussi chargée d'informer les transporteurs aériens ainsi que les agences et opérateurs de voyages sur la qualité de la transmission des données. Cette unité se trouve sous l'autorité d'un agent du ministère de l'Intérieur, secondé par un directeur adjoint venant du ministère en charge des douanes, dont les fonctions sont détaillées à l'article 4 du décret n° 2014-1566, modifié par le décret n° 2018-722.

¹⁵¹⁰ Organisation mondiale des douanes, Lignes directrices à l'intention des administrations des douanes – Comment mettre au point un programme de renseignements préalables concernant les voyageurs (RPCV) / de dossiers passagers (PNR), juillet 2017, Annexe III au doc. PS0067F, p. III/15

¹⁵¹¹ Liste des unités d'informations passagers visées à l'article 4 de la directive (UE) 2016/681 du Parlement européen et du Conseil 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 : JOUE n° C 230, 2 juillet 2018, p. 6

¹⁵¹² V. CORREA, « Fasc. 978 : Données des passagers aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

D'après l'article 4 de la directive PNR, l'UIP est fonctionnellement indépendante des autres autorités nationales habilitées à demander ou recevoir ces données, car ces dernières doivent passer par elle pour les obtenir. Cela s'explique par « la nécessité d'empêcher que ces informations ne circulent entre les divers services de sécurité pour des raisons autres que celles décrites par la directive, comme c'est par exemple le cas aux États-Unis d'Amérique »¹⁵¹³.

L'article 7 de la directive impose également aux États membres d'établir une liste des autorités compétentes autorisées à demander des données des dossiers passagers à l'unité ou à en recevoir de sa part. Afin de limiter le nombre d'autorités potentielles, la directive entend que celles-ci soient « des autorités compétentes en matière de prévention ou de détection des infractions terroristes ou des formes graves de criminalité, ainsi que d'enquêtes ou de poursuites en la matière »¹⁵¹⁴. Cependant, les États membres utilisent différemment cette capacité de désignation. L'Italie, par exemple, a désigné les Carabiniers, la police, la garde des finances (police financière et douanière) et la police pénitentiaire tandis que la France a quant à elle fixé une liste de dix-sept autorités qui a été communiquée à la Commission européenne¹⁵¹⁵.

Cette dernière comprend la direction centrale de la police judiciaire ; la direction centrale de la police aux frontières ; la direction centrale de la sécurité publique ; le centre de veille de la direction de la coopération internationale ; l'unité de coordination de la lutte antiterroriste ; la direction générale de la sécurité intérieure ; la direction des opérations et de l'emploi de la direction générale de la gendarmerie nationale ; le pôle judiciaire de la gendarmerie nationale ; la gendarmerie départementale ; les gendarmeries spécialisées ; la direction nationale du renseignement et des enquêtes douanières ; le service national de la douane judiciaire ; les services chargés de la coordination locale des unités douanières ; les services territoriaux chargés de l'orientation des contrôles ; la direction générale de la sécurité extérieure ; la direction du renseignement et de la sécurité de la défense ; la direction du renseignement militaire¹⁵¹⁶.

¹⁵¹³ R. BRETT, « La directive "PNR" du 27 avril 2016, nouvelle étape de la politique européenne de lutte contre la criminalité », *Protection des données personnelles*, Europe, étude 1, spéc. p. 3, 2017.

¹⁵¹⁴ Directive (UE) 2016/681, 27 avril 2016, article 7, § 2.

¹⁵¹⁵ Liste des autorités compétentes visées à l'article 7 de la 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 : JOUE n° C 194, 6 juin 2018, p. 1-8.

¹⁵¹⁶ V. CORREA, « Fasc. 978 : Données des passagers aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

Néanmoins, l'article R. 232-15 du Code de la sécurité intérieure distingue les entités habilitées à formuler des requêtes à l'UIP et à être destinataires des réponses, d'une part, et les entités seulement habilitées à être destinataires des données. Ces entités varient, quelquefois marginalement, selon l'objet même de l'utilisation des données.

La législation américaine permet au Service des douanes et de la protection des frontières de transférer les données PNR avec d'autres agences fédérales mais uniquement aux fins de garantir la sécurité nationale¹⁵¹⁷. Le partage d'informations se fait conformément aux règles établies par le département de la sécurité intérieure en respectant le droit applicable et notamment les traités internationaux conclus par les États-Unis dans ce domaine. Le ministère de l'Intérieur américain insiste sur le fait que les données des dossiers passagers ne peuvent être transmises que de façon ponctuelle, lorsque des besoins spécifiques sont démontrés pour garantir la sécurité intérieure et sous réserve que ces informations soient suffisamment protégées¹⁵¹⁸.

b. Le transfert à des autorités publiques d'États tiers, un encadrement juridique au défi d'échanges transfrontaliers diversifiés

Le droit européen vise à « imposer la création et la gestion de vingt-huit systèmes de collecte standardisés, correspondants à chacun des vingt-sept États membres de l'Union européenne » au lieu de mettre en place un fichier central de données des dossiers passagers¹⁵¹⁹. L'échange de données de passagers entre États membres a de fait une importance fondamentale pour garantir la sécurité sur l'ensemble de l'espace de l'Union européenne.

L'article 9 de la directive PNR encadre le transfert des données des dossiers passagers entre UIP des États membres. Ainsi, lorsqu'une UIP traite des données des passagers aériens et identifie une ou des personnes suspectées d'infraction terroriste ou d'une forme grave de criminalité, elle devra transférer les données des passagers ou le résultat du traitement de celles-ci aux UIP des autres États membres, lesquelles devront les transmettre à leurs autorités compétentes¹⁵²⁰.

¹⁵¹⁷ Article 19 CFR § 122.49d, (d).

¹⁵¹⁸ V. CORREA, « Fasc. 978 : Données des passagers aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

¹⁵¹⁹ R. BRETT, « La directive "PNR" du 27 avril 2016, nouvelle étape de la politique européenne de lutte contre la criminalité », *Protection des données personnelles*, Europe, étude 1, spéc. p. 3, 2017.

¹⁵²⁰ Directive (UE) 2016/681, 27 avr. 2016, article 9, § 1.

Parallèlement, une UIP peut demander à une autre UIP la transmission de données non encore anonymisées ou le résultat du traitement de celles-ci¹⁵²¹. Dûment motivée, la demande ne peut toutefois concerner que les cas de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière. La directive aspire en conséquence à permettre la coopération des unités d'information, en réseau, tout en évitant que des requêtes soient transmises pour d'autres fins que la lutte contre les infractions terroristes ou la criminalité grave, comme cela pourrait être particulièrement le cas en matière de lutte contre l'évasion fiscale¹⁵²². Cela explique aussi pourquoi les autorités compétentes désignées sur le plan national ne peuvent s'adresser à l'unité d'un autre État membre que dans les cas d'urgence et seulement à des fins visées à l'article 1^{er}, paragraphe 2 de la directive¹⁵²³.

Enfin, dans des cas considérés comme exceptionnels, une UIP peut demander à une autre d'un autre État membre européen de solliciter des données PNR auprès d'une société aérienne, en dehors des séquences prévues de transfert, selon l'article 9, paragraphe 4 de la directive PNR. Europol peut aussi, sous certaines conditions, demander aux UIP des États membres des données des passagers aériens ou le résultat du traitement de celles-ci, d'après l'article 10 de la directive¹⁵²⁴. En France, les articles R. 232-16 à R. 232-18 du Code de la sécurité intérieure prévoient les procédures de communication et de réception des données à caractère personnel des voyageurs aux UIP d'autres États membres, aux autorités compétentes dans des cas prédéfinis, ainsi qu'à Europol.

Étant donné l'extrême sensibilité qui entoure les enjeux du transfert des données des dossiers passagers vers des pays tiers, l'article 11 de la directive PNR adopte une approche prudente, puisqu'il insiste sur le transfert de données au cas par cas, sans se montrer très précis. Ledit article énonce, en effet, que les conditions prévues à l'article 13 de la décision-cadre 2008/977/JAI, doivent être respectées, alors que cette décision-cadre a été abrogée le jour même de l'adoption de la directive européenne 2016/680 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.

¹⁵²¹ Ibidem, article 9, § 2.

¹⁵²² V. CORREA, « Fasc. 978 : Données des passagers aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

¹⁵²³ Directive (UE) 2016/681, précit., article 9, § 3.

¹⁵²⁴ V. CORREA, « Fasc. 978 : Données des passagers aériens », *LexisNexis*, JurisClasseur Communication, 15 novembre 2019.

Vincent Correa estime que les conditions encadrant le transfert des données doivent se baser sur la directive (UE) 2016/680 dans la mesure où l'article 59 de la directive (UE) 2016/680 fait référence à la décision-cadre 2008/977/JAI. Les dispositions pertinentes concernant les transferts sur la base d'une décision d'adéquation et les transferts de données à caractère personnel à des destinataires établis dans des pays tiers se trouvent respectivement aux articles 36 et 39 de la directive (UE) 2016/680. Le chercheur considère que les transferts des dossiers passagers doivent se fonder sur l'article 39 de la directive et, le cas échéant, sur la base d'une décision d'adéquation. Les conditions nécessaires sont les suivantes : le transfert envisagé doit avoir pour unique objet la prévention et la détection des infractions terroristes et des formes graves de criminalité ; le pays tiers ne doit pas accepter de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire ; les conditions de l'article 9, § 2 de la directive (relatif au transfert entre UIP d'États membres) doivent être respectées¹⁵²⁵.

L'article 11, paragraphe 2 de la directive européenne 2016/681 soumet le transfert des données des dossiers passagers sans l'accord préalable de l'État dans lequel elles ont été obtenues à des conditions plus restrictives que celles établies à l'article 35, paragraphe 2 de la directive 2016/680. Toutefois, la directive PNR s'applique « sans préjudice des obligations et engagements d'États membres ou de l'Union qui découlent d'accords bilatéraux ou multilatéraux avec des pays tiers »¹⁵²⁶, permettant ainsi des transferts facilités avec certains autres pays partenaires. En France, l'article R. 232-19 du Code de la sécurité intérieure autorise le transfert des données personnelles et du résultat du traitement de celles-ci à des autorités d'États tiers, au cas par cas et seulement si les conditions également applicables au transfert vers des autorités d'autres États membres de l'Union européenne sont remplies.

Le transfert de données PNR a ainsi soulevé plusieurs préoccupations, car ces données contenaient des données dites sensibles. Or, les usagers du transport aérien devaient voir leur droit au respect de la vie privée et à la protection des données à caractère personnel respecté. Le partage avec des agences gouvernementales, en particulier au-delà des frontières de l'Union européenne qui dispose d'un cadre juridique protecteur¹⁵²⁷, soulève ainsi des inquiétudes quant à la manière les données sont utilisées, stockées et in fine protégées. Il existe, en effet, un risque d'accès non autorisé, de violation de données et d'utilisation abusive des données personnelles, en violation avec les droits fondamentaux des citoyens européens.

¹⁵²⁵ Ibidem

¹⁵²⁶ Ibid.

¹⁵²⁷ C. BILLET, « L'échange et la protection de données avec les États tiers : un nouveau volet prioritaire de l'action extérieure de l'Union ? », *RTDEur.*, Dalloz, n° 3, p. 689, 2020.

Le transfert de données PNR implique des complexités juridiques et juridictionnelles. Différents pays ont des lois différentes concernant la protection des données à caractère personnel, la protection de la vie privée et le partage et le transfert des données. Veiller à ce que le transfert de données PNR soit conforme aux cadres juridiques pertinents peut s'avérer difficile et des désaccords peuvent survenir concernant la juridiction et les lois applicables.

Ces préoccupations ont conduit à des débats¹⁵²⁸ et à des différends entre les gouvernements, les compagnies aériennes, les défenseurs de la vie privée et les organisations de défense des droits de l'Homme¹⁵²⁹. Des efforts ont été réalisés pour établir des accords et des cadres internationaux, tels que des réglementations sur la protection des données et des accords bilatéraux ou multilatéraux, afin de résoudre ces problèmes et de trouver un équilibre entre les besoins de sécurité¹⁵³⁰ et le droit à la vie privée. Cependant, trouver un consensus sur ces questions reste un défi de taille.

Le transfert des données des dossiers passagers entre l'Union européenne et les États-Unis a ainsi fait l'objet de controverses¹⁵³¹ et d'un litige juridique¹⁵³² pour diverses raisons dont la protection des données à caractère personnel puisque l'Union dispose de règles plus strictes en la matière, notamment le RGPD visant à protéger la vie privée et les données personnelles des citoyens européens.

Le transfert de données PNR aux États-Unis, où les lois sur la protection des données sont perçues comme plus faibles¹⁵³³, a soulevé des inquiétudes quant à l'adéquation des garanties et au potentiel d'utilisation abusive ou d'accès non autorisé aux informations personnelles¹⁵³⁴. Par ailleurs, le droit européen a insisté sur des limitations claires à l'utilisation des données PNR transférées aux États-Unis¹⁵³⁵. Aussi, les autorités européennes ont exprimé des

¹⁵²⁸ E. CARPANELLI, N. LAZZERINI, "PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU", *Air and Space Law*, 2017.

¹⁵²⁹ K. BIEDENKOPF, O. COSTA, M. GÓRA, "Introduction: shades of contestation and politicization of CFSP", *European Security*, 2021, pp. 325-343.

¹⁵³⁰ J. JEANDESBOZ, "Ceci n'est pas un contrôle: PNR Data Processing and the Reshaping of Borderless Travel in the Schengen Area", *European Journal of Migration and Law*, 2021.

¹⁵³¹ S. PEYROU, « De l'accord PNR à Prism, bilan et perspectives sur les malentendus transatlantiques : lutte anti-terroriste versus protection des données personnelles », *GDR-ELSJ*, 11 septembre 2013.

¹⁵³² CJCE, 30 mai 2006, Parlement c/ Conseil.

¹⁵³³ S. LE STRUJON, « Le California Consumer Privacy Act : premier pas vers un RGPD américain ? », *Revue de l'Union européenne*, Dalloz, 2020 ; A. ADAM, « L'échange de données à caractère personnel entre l'Union européenne et les États-Unis », *Revue de droit européen*, Dalloz, 2006, p. 411.

¹⁵³⁴ G. HORNING, F. BOEHM, "Comparative Study on the 2011 Draft Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security", *The Greens, European Free Alliance*, Passau/Luxembourg, 14 mars 2012.

¹⁵³⁵ Directive (UE) PNR, article 1, alinéa 2. Cette disposition rappelle que les données recueillies ne sont traitées qu'à des fins de lutte contre le terrorisme et les formes graves de criminalité.

inquiétudes¹⁵³⁶ quant à une dérive potentielle : des données collectées dans un but spécifique, comme la lutte contre le terrorisme, pourraient être utilisées pour d'autres activités, notamment de renseignement. L'Union européenne a ainsi souhaité assurer le strict respect du principe de limitation des finalités en veillant à ce que les données ne soient utilisées qu'aux fins pour lesquelles elles ont été initialement collectées¹⁵³⁷.

Un autre problème a été le manque de recours judiciaire adéquat pour les citoyens de l'Union européenne dont les données sont mal traitées ou utilisées à mauvais escient par les autorités américaines. Les citoyens européens attendant des voies de recours et des mécanismes efficaces pour contester les décisions fondées sur leurs données PNR, l'Union européenne a demandé des garanties plus solides de recours et de procédure régulière pour ses citoyens lorsque leurs données sont transférées aux États-Unis¹⁵³⁸.

Enfin, l'application extraterritoriale des lois américaines, en particulier dans le domaine de la sécurité nationale et du renseignement, a suscité des inquiétudes au sein de l'Union européenne : l'accès potentiel aux données PNR des agences de renseignement américaines sans garanties ou surveillance appropriées a été un point litigieux, car cela peut porter atteinte aux droits fondamentaux des citoyens européens¹⁵³⁹. Ces problèmes ont conduit à des contestations juridiques¹⁵⁴⁰ et à des négociations entre l'Union européenne et les États-Unis pour établir des cadres garantissant la protection des données personnelles tout en permettant le transfert de données PNR à des fins légitimes de sécurité. Les négociations ont abouti à des accords PNR entre les deux pays qui visent à trouver un équilibre entre les besoins de sécurité et le droit à la vie privée. Toutefois, le transfert de données PNR reste un sujet d'examen et de débat permanents.

D'autres sujets ont également fait l'objet de débats comme la transparence et la responsabilité dans le cadre des processus de transfert des données PNR. En effet, les parties prenantes, y

¹⁵³⁶ Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure, 9 février 2012.

¹⁵³⁷ Directive (UE) PNR, article 1, alinéa 2.

¹⁵³⁸ Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure, 9 février 2012.

¹⁵³⁹ S. PEYROU-PISTOULEY, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », *Europe actualité du droit communautaire*, 2012.

¹⁵⁴⁰ M. PRIVAL, « L'accord PNR approuvé sans grand engouement par le Parlement européen », *Le Taurillon*, 2012, en ligne à URL : <https://www.taurillon.org/L-accord-PNR-approuve-sans-grand-engouement-par-le-Parlement-europeen,04947> consulté le 13 juillet 2023.

compris les gouvernements, les compagnies aériennes et les défenseurs de la protection de la vie privée et de la protection des données personnelles, ont engagé des discussions sur la transparence des pratiques de collecte de données, les finalités pour lesquelles celles-ci sont utilisées et les mécanismes de surveillance en place pour assurer une responsabilité effective dans le cadre de leur traitement¹⁵⁴¹.

Pour améliorer la protection des données transférées, plusieurs recommandations pourraient être faites. Tout d'abord, la mise en place de normes strictes sur la protection des données : en mettant en œuvre et en appliquant des lois et réglementations solides sur la protection des données qui établissent des exigences claires pour la collecte, le stockage et le transfert des données PNR. Ces normes devraient accorder la priorité aux droits à la vie privée, au consentement, à la minimisation des données, à la limitation des finalités et au principe de proportionnalité. Aussi, le législateur doit offrir des garanties adéquates afin de veiller à ce que des mesures techniques et organisationnelles appropriées soient appliquées pour protéger les données PNR.

Les États doivent également favoriser des accords et normes internationaux en matière de transfert des données PNR qui respectent les droits à la vie privée et à la protection des données personnelles en fournissant des lignes directrices cohérentes à toutes les juridictions. Ces accords devraient aborder des questions telles que les conflits de compétence, l'application extraterritoriale des lois et la protection des droits individuels. Les législateurs doivent également veiller à ce que les personnes disposent de recours et de mécanismes judiciaires efficaces en cas de mauvaise manipulation, d'accès non autorisé ou d'utilisation abusive de leurs données PNR. Cela inclut la possibilité de contester les décisions fondées sur les données PNR et de demander réparation en cas de violation de leurs droits. Aussi, les autorités compétentes doivent effectuer des audits et des évaluations périodiques des pratiques de protection des données des organisations impliquées dans le transfert de données PNR. Cela permet d'identifier les vulnérabilités, d'assurer la conformité et de maintenir un niveau élevé de protection des données. La mise en œuvre de ces recommandations peut contribuer à une meilleure protection des données PNR transférées, en permettant un équilibre entre les besoins de sécurité et les droits individuels à la vie privée.

¹⁵⁴¹ S. PEYROU-PISTOULEY, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », *Europe actualité du droit communautaire*, 2012.

Section 2 – Le stockage des dossiers passagers : une fragile limitation temporelle au profit de la conservation des données personnelles des passagers aériens

La conservation des données des dossiers passagers a suscité des polémiques en raison de préoccupations concernant la protection de la vie privée, la sécurité des données et les droits individuels (sous-section 1). En effet, ces données peuvent être utilisées à des fins autres que celles pour lesquelles elles ont été initialement collectées, ce qui soulève des inquiétudes quant à leur utilisation abusive. Les craintes d'utilisation commerciale des données personnelles à des fins de marketing ciblé ou de profilage des passagers ont été soulevées. En raison de ces préoccupations, certaines organisations de défense des droits de l'Homme et de la vie privée¹⁵⁴², ainsi que la CJUE¹⁵⁴³, ont remis en question la conservation des données PNR et ont appelé à une meilleure protection des droits individuels tout en maintenant un équilibre avec les besoins légitimes de sécurité et de gestion opérationnelle des compagnies aériennes (sous-section 2). Cette incapacité à maîtriser de manière concrète la conservation de ces données est l'une des autres facettes de l'affaiblissement du territoire en tant que réalité juridique contraignante.

Sous-section 1 – La conservation des données à caractère personnel, un enjeu crucial pour le droit européen

La gestion de la durée de conservation des données à caractère personnel est aujourd'hui un élément central en droit européen, notamment dans le RGPD, tant au regard du respect des obligations juridiques du responsable de traitement que pour la protection de la vie privée des personnes concernées.

§ 1 – La conservation des données à caractère personnel, un enjeu contemporain pour les entités publiques et privées

La conservation de données à caractère personnel en droit se réfère à l'acte de stocker, maintenir ou conserver des informations qui peuvent être utilisées pour identifier directement

¹⁵⁴² CJUE, arrêt de la Cour dans l'affaire Ligue des droits humains, C-817/19, 21 juin 2022. En 2017, la Ligue des droits humains (LDH) avait saisi la Cour constitutionnelle belge au motif que la directive PNR ne respectait pas le droit au respect de la vie privée et à la protection des données à caractère personnel. Voir en ce sens : X. DELPECH, « La directive PNR confrontée au respect des droits fondamentaux », *Dalloz, Revue trimestrielle de droit commercial*, 19 septembre 2022. Lire également l'avis du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, « Avis sur les implications en matière de protection des données du traitement des dossiers passagers », Conseil de l'Europe, 19 août 2016.

¹⁵⁴³ CJUE, op. cit.

ou indirectement une personne physique¹⁵⁴⁴. Il s'agit d'une activité encadrée par de nombreuses législations nationales ou supranationales. Dans le cadre de la législation européenne sur la protection des données, la conservation des données à caractère personnel est soumise à plusieurs principes et obligations. Concernant la durée de conservation des données, il est énoncé que les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour atteindre la finalité pour laquelle elles ont été collectées. La durée de conservation peut varier en fonction de la nature des données, du contexte et des exigences légales ou réglementaires applicables¹⁵⁴⁵.

Le traitement des données à caractère personnel comprend plusieurs étapes successives. La CNIL parle de « cycle de vie » de la donnée personnelle qui connaît trois phases¹⁵⁴⁶. La première phase est celle de la conservation en base active d'une durée nécessaire à la réalisation de la finalité du traitement, autrement dit de l'objectif ayant justifié la collecte des données. En général, ces données sont facilement accessibles dans l'environnement de travail immédiat pour les services opérationnels qui ont la charge de ce traitement¹⁵⁴⁷. La deuxième phase est celle de l'archivage intermédiaire, lorsque les données ne sont plus utilisées pour atteindre un objectif fixé. Toutefois, elles présentent encore un intérêt administratif pour l'organisme, comme la gestion d'un éventuel litige, ou bien doivent être conservées pour répondre à une obligation légale. Ces données peuvent être consultées de façon ponctuelle et motivée par des personnes spécifiquement habilitées. La troisième phase est celle de l'archivage définitif. En raison de leur intérêt et de leur valeur, certaines informations font l'objet d'un archivage définitif et pérenne. Contrairement à la conservation de base active, les deux dernières étapes ne sont pas systématiquement appliquées. Leur nécessité doit être évaluée pour chaque traitement. Pour chacune de ces phases, un tri sera opéré pour les données.

Les aéroports conservent les données à des fins similaires à celles des transporteurs aériens mais également pour gérer efficacement les opérations aéroportuaires et assurer la sécurité des passagers et des installations. En effet, les aéroports sont des lieux sensibles en matière de sécurité et la conservation des données y est essentielle pour identifier les passagers et le

¹⁵⁴⁴ L'article 5 du RGPD oblige chaque responsable de traitement à déterminer une durée de conservation des données à caractère personnel cohérente et justifiée au regard de l'objectif de leur traitement. Voir : A. BERY, L. DELPRAT, « Les nouveaux délais de conservation des dossiers médicaux », *Art*, 2008.

¹⁵⁴⁵ RGPD, article 5. Voir également : article 4 alinéa 5 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

¹⁵⁴⁶ CNIL, « Les durées de conservation des données », 28 juillet 2020, en ligne à URL : <https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees> consulté le 18 juillet 2023.

¹⁵⁴⁷ Ibidem

personnel autorisé, vérifier leur conformité aux réglementations de sécurité, contrôler l'accès aux zones restreintes ainsi que détecter toute activité suspecte ou menace potentielle. L'enjeu est sécuritaire et n'est pas négligeable. Aussi, ces données sont essentielles dans le contrôle des frontières dans la mesure où dans de nombreux pays, les aéroports sont les principaux points d'entrée pour les voyageurs internationaux. Les aéroports conservent les données des passagers pour faciliter le contrôle des frontières, assurer le respect des visas et des permis de séjour mais aussi s'assurer que les voyageurs remplissent les conditions requises pour entrer sur un territoire national.

Par ailleurs, les plateformes aéroportuaires¹⁵⁴⁸ doivent planifier et gérer efficacement les mouvements des avions sur les pistes, l'utilisation des portes d'embarquement, la disponibilité des ressources au sol, tels que les chariots à bagages, les escaliers, les passerelles et les ressources humaines. La conservation des données permet une coordination efficace pour éviter les retards et les congestions. Il en est de même pour la gestion quotidienne des voyages sachant que les aéroports doivent conserver ces données pour les horaires de vol, les retards, les annulations, les débarquements, les décollages, les mouvements d'avions et les opérations au sol. Ces informations sont utilisées pour garantir un fonctionnement fluide de l'aéroport.

Toutefois, certaines compagnies aériennes stockent des données des dossiers passagers dans des systèmes qui pourraient ne pas être suffisamment sécurisés, une pratique qui expose ces données à des risques de piratage ou de vol de données. Les atteintes à la sécurité peuvent entraîner des conséquences graves pour la vie privée des passagers. La grande décision dans le domaine de la protection des données personnelles des passagers aériens concerne British Airways qui a été condamnée, en octobre 2020¹⁵⁴⁹, par l'Information Commissioner's Office (ci-après ICO), l'autorité en charge de la protection des données personnelles en Grande-Bretagne, à payer 20 millions de livres sterling pour manquement à la protection des données de passagers. Ce cybercrime a eu lieu en 2018 et les données volées comprenaient des informations de connexion, sur des cartes de paiement, les détails des réservations de voyage ainsi que les noms et adresses de voyageurs. Plus de 400 000 clients de la compagnie étaient concernés. L'amende finalement imposée était considérablement inférieure aux 183 millions

¹⁵⁴⁸ Aéroport de Lyon, Politique de protection des données, 9 juillet 2020, en ligne à URL : https://www.lyonaeroports.com/sites/default/files/2020-07/politique_donnees_personnelles_20200709.pdf consulté le 20 juillet 2023.

¹⁵⁴⁹ ICO, Penalty notice, COM0783542, British Airways pie, en ligne à URL : <https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf> consulté le 20 juillet 2023.

que l'ICO avait initialement annoncé en 2019. L'enquête des autorités britanniques avait conclu que les mesures de sécurité requises n'étaient pas en place à l'époque¹⁵⁵⁰.

Le piratage ayant pris fin avant le Brexit en septembre 2018, l'ICO a pu appliquer le RGPD en infligeant de lourdes amendes aux entreprises dont les systèmes de défense informatiques étaient insuffisamment forts pour empêcher les violations de données. Aussi, l'ICO a sanctionné l'entreprise au nom de tous les pays de l'Union européenne, dont la France, en raison de fuites impliquant des ressortissants européens, un mécanisme également prévu par le RGPD. La facture aurait pu être plus élevée, car l'ICO avait rappelé que l'amende ne couvrait que les quelques semaines entre le début du RGPD en mai 2018 et la détection d'une cyberattaque alors que la première attaque contre des données personnelles remontait à 2014¹⁵⁵¹.

Cette sanction illustre l'importance du RGPD dans le domaine de la cybercriminalité. Cette législation européenne a fait de la sécurité des données une exigence générale à respecter et a créé des obligations contraignantes en la matière. Les manquements peuvent ainsi en principe être sanctionnés jusqu'à 10 millions d'euros d'amende ou 2 % du chiffre d'affaires mondial¹⁵⁵². En cas de récidive, les sanctions prévues par le RGPD peuvent être considérablement aggravées. Le montant de l'amende peut atteindre jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial de l'entreprise, le montant le plus élevé étant retenu¹⁵⁵³. Cette augmentation des sanctions vise à dissuader les entreprises de réitérer leurs infractions aux règles de protection des données personnelles.

Par ailleurs, cette décision confirme que la sécurité des données nécessite une vigilance permanente, tout particulièrement pour ce type d'opérateur, avec de lourdes conséquences en cas d'infractions. Enfin, elle positionne le droit européen et les autorités de protection des données comme des acteurs efficaces et à part entière de la cybersécurité, en invitant les entités traitant des données personnelles à une sérieuse gestion de leur patrimoine informationnel. Par conséquent, toutes les entités qui traitent des données à caractère

¹⁵⁵⁰ ICO, Penalty notice, COM0783542, British Airways pie, en ligne à URL : <https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf> consulté le 20 juillet 2023.

¹⁵⁵¹ Le Monde, « British Airways et Marriott écotent de lourdes amendes pour des données personnelles mal sécurisées », *Pixels*, Vie privée, 2 novembre 2020, en ligne à URL : https://www.lemonde.fr/pixels/article/2020/11/02/british-airways-et-marriott-ecotent-de-lourdes-amendes-pour-des-donnees-personnelles-mal-securisees_6058212_4408996.html consulté le 20 juillet 2023.

¹⁵⁵² RGPD, article 83, alinéa 4. Voir en ce sens : CNIL, « Cybersécurité : l'autorité britannique de protection des données, en coopération avec la CNIL, inflige deux amendes record », 2 novembre 2020, en ligne à URL : <https://www.cnil.fr/fr/cybersecurite-ico-en-cooperation-avec-la-cnil-inflige-amendes-record> consulté le 20 juillet 2023.

¹⁵⁵³ RGPD, article 83, alinéa 5.

personnel doivent établir des mesures pour prévenir les attaques cybercriminelles visant les données et réagir de manière appropriée et rapide en cas d'incident. Les obligations prévues par le RGPD tendent à éviter qu'une attaque cybercriminelle cause des préjudices aux entités comme aux personnes concernées.

§ 2 – La protection nécessaire des données par le droit européen à travers le principe de la limitation de la durée de conservation

Le droit européen énonce un principe de limitation de la durée de conservation qui implique que les données à caractère personnel soient supprimées ou anonymisées lorsqu'elles ne sont plus nécessaires pour les finalités pour lesquelles elles ont été collectées. L'article 5, paragraphe 1, point e) du RGPD et l'article 5, paragraphe 4, point e) de la Convention 108 modernisée s'accordent sur le principe selon lequel les données personnelles doivent être conservées de manière à permettre l'identification des personnes concernées uniquement pour une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. Les données à caractère personnel doivent donc être effacées ou anonymisées lorsque ces finalités ont été réalisées. Afin de s'assurer que les données ne sont pas conservées plus longtemps que nécessaire, « des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique »¹⁵⁵⁴.

Dans l'affaire *S. et Marper*¹⁵⁵⁵, la Cour européenne des droits de l'homme (ci-après CEDH) avait conclu que les principes fondamentaux du Conseil de l'Europe, tout comme le droit et la pratique des Parties contractantes, imposent que la conservation des données personnelles soit proportionnée à l'objet de la collecte et limitée dans le temps, notamment dans le domaine de la police. La Cour de Strasbourg a considéré en l'espèce que la conservation illimitée des échantillons cellulaires, des empreintes digitales et des profils ADN des deux demandeurs était inutile et disproportionnée dans une société démocratique puisque la procédure pénale contre eux s'était conclue, respectivement, par un acquittement et une décision de classement sans suite.

Toutefois, la limitation de la durée de conservation des données personnelles ne s'applique qu'aux données conservées sous une forme permettant l'identification de la personne concernée. Par conséquent, les données qui ne sont plus nécessaires peuvent être légalement

¹⁵⁵⁴ Europa, *Manuel de droit européen en matière de protection des données*, Principes clés du droit européen en matière de protection des données, 2018.

¹⁵⁵⁵ CEDH, Cour (Quatrième Section), *S. et Marper c/ c. Royaume-Uni*, 16 janvier 2007, n° 30562/04, 30566/04. Voir en ce sens : R. BELLANOVA, P. DE HERT, « Le cas *S. et Marper* et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », *Cultures & conflits*, 2009, pp. 101-114.

conservées en anonymisant les données. Les données archivées à des fins d'intérêt public, à des fins scientifiques ou historiques ou à des fins statistiques peuvent être conservées plus longtemps à la condition qu'elles soient utilisées exclusivement à ces fins. Des mesures techniques et organisationnelles appropriées doivent être prises pour le stockage et l'utilisation continus des données personnelles afin de protéger les droits et libertés des personnes concernées.

La Convention 108 modifiée envisage également des exceptions au principe de limitation de la durée de conservation, à la condition que ces exceptions soient prévues par la loi, respectent le contenu essentiel des libertés et droits fondamentaux et constituent des mesures nécessaires et proportionnées pour atteindre un nombre limité d'objectifs légitimes. Ces exceptions comprennent, entre autres, la protection de la sécurité nationale, la recherche et la poursuite d'infractions pénales, l'exécution de sanctions pénales, la protection des personnes concernées et la sauvegarde des libertés et droits fondamentaux d'autrui.

Dans l'affaire *Digital Rights Ireland* de 2014¹⁵⁵⁶, la CJUE a examiné la validité de la directive 2006/24/CE sur la conservation des données¹⁵⁵⁷ qui vise à harmoniser les dispositions nationales applicables à la conservation des données à caractère personnel générées ou traitées par les services ou réseaux publics de communications électroniques afin de lutter contre les infractions graves telles que le crime organisé et le terrorisme. La directive sur la conservation des données exige que les données soient conservées « d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées »¹⁵⁵⁸. La CJUE a également noté que la directive ne fait aucune mention de critères objectifs pour déterminer la durée exacte de conservation des données, allant d'un minimum de six mois à un maximum de vingt-quatre mois ; de tels critères pourraient permettre de s'assurer qu'elle soit limitée au strict nécessaire.

Cet arrêt est important, car il a eu un impact significatif sur la protection des droits fondamentaux des citoyens européens en matière de protection des données personnelles, de vie privée et de lutte contre la surveillance de masse. En invalidant la directive sur la conservation des données, les juges européens ont envoyé un signal sérieux aux États membres européens en affirmant que la surveillance de masse sans justification appropriée et

¹⁵⁵⁶ CJUE, Grande Chambre, *Digital Rights Ireland Ltd et autres*, 8 avril 2014, aff. jointes C-293/12 et C-594/12.

¹⁵⁵⁷ Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54).

¹⁵⁵⁸ Ibidem.

sans limites adéquates n'était pas compatible avec les principaux de la démocratie et les droits fondamentaux.

Précisément, l'arrêt affirma que la conservation généralisée et indifférenciée des données de communication des citoyens européens était une violation grave de leur droit fondamental à la vie privée, tel que protégé par la Charte des droits fondamentaux de l'Union européenne, renforçant ainsi la protection de la vie privée des citoyens dans un environnement numérique en pleine mutation. Cette décision a renforcé les notions fondamentales comme la vie privée et la protection des données à caractère personnel qui doivent être prises en compte dans la régulation des communications électroniques et de la sécurité nationale.

En jouant un rôle clé dans la protection des droits numériques des citoyens européens, l'arrêt Digital Rights Ireland, du nom de l'organisation de défense des droits numériques, a entraîné des conséquences sur la façon dont l'Union européenne aborde les enjeux de protection des données à caractère personnel. L'Union européenne et les autorités nationales européennes aspirent ainsi à offrir un cadre harmonisé, pionnier et conscient de tous les enjeux afin de protéger les citoyens européens. L'extraterritorialité de l'acte législatif est ici importante, car le RGPD s'applique à tous les opérateurs, qu'ils soient étrangers ou européens, dès lors qu'ils manipulent des données relatives à des citoyens européens. Contrairement aux critiques de certaines sociétés, le législateur européen a évité la distorsion de concurrence¹⁵⁵⁹. Pour ses défenseurs, ce règlement a pour objet initial de lutter contre le risque de concurrence déloyale en visant les conglomerats monopolistiques agrégateurs de données personnelles sachant que l'utilisation des nouvelles technologies, notamment dans le domaine de la sécurité, par exemple la reconnaissance faciale, porte toujours un risque pour les libertés et droits fondamentaux de l'utilisateur¹⁵⁶⁰.

Les défenseurs de la protection des données personnelles ont regretté que l'application du RGPD présente encore de sérieuses lacunes notamment quant à l'application des grands principes affirmés par le législateur européen, car certains juges nationaux semblent chercher par tous les moyens à éviter de traiter un dossier relatif au RGPD¹⁵⁶¹.

¹⁵⁵⁹ C. EBERLE, « RGPD ou l'Europe qui innove, protège, et influence », *Les Echos*, 22 octobre 2018, en ligne à URL : <https://www.lesechos.fr/idees-debats/cercle/opinion-rgpd-ou-leurope-qui-innove-protège-et-influence-142493> consulté le 19 juillet 2023.

¹⁵⁶⁰ S. PERYOU-BARTOLL, « Nouvelles technologies, sécurité et protection des données à caractère personnel : un cadre juridique européen à la hauteur des enjeux ? », *Cahiers de la sécurité et de la justice*, 2022, pp.186-196.

¹⁵⁶¹ Le Monde, « Max Schrems : 'Le RGPD a une influence parce qu'il est et continuera d'être le standard mondial' », 25 mai 2023, en ligne à URL : <https://www.lemonde.fr/pixels/article/2023/05/25/max-schrems-le->

Sous-section 2 – La conservation des données des passagers aériens, un équilibre entre sécurité et liberté difficilement mis en œuvre

L'utilisation des données des dossiers passagers a soulevé des préoccupations en matière de protection des données à caractère personnel et de respect de la vie privée des passagers. Des questions se posent quant à la proportionnalité de la collecte et de l'utilisation de ces données, la durée de conservation, les mesures de sécurité mises en place, l'accès aux données par les autorités compétentes ainsi que les garanties et les recours disponibles pour les individus concernés.

§ 1 – La conservation des données des passagers aériens, un nouvel enjeu contemporain pour les acteurs du transport aérien

Les transporteurs aériens conservent les données PNR pour des raisons de sécurité, de gestion opérationnelle, de conformité aux réglementations et de services aux passagers. D'abord, du point de vue de la sécurité, ils contiennent des informations essentielles sur les passagers. Ces informations sont nécessaires pour identifier les passagers et faciliter la sécurité aérienne. En cas d'urgence ou d'incident, elles peuvent être utilisées pour localiser rapidement les passagers et les informer en cas de changements ou d'annulations de vol.

Ensuite, dans le cadre de la gestion opérationnelle, les données PNR sont utilisées pour gérer les opérations aériennes, notamment en termes de planification des vols, de répartition des sièges, de gestion des réservations et de gestion des surréservations. Ces informations aident également les compagnies aériennes à anticiper la demande, à optimiser les ressources et à améliorer l'efficacité globale de leurs opérations. Par ailleurs, les transporteurs aériens sont soumis à des réglementations strictes en matière de sécurité et d'immigration. Ils sont tenus de conserver les données des passagers conformément aux lois et aux réglementations en vigueur dans les pays où ils opèrent. Ces données peuvent être requises par les autorités compétentes pour des raisons de sécurité nationale ou pour faciliter les contrôles aux frontières.

Aussi, les données PNR permettent aux compagnies aériennes de fournir un meilleur service client en anticipant les besoins des passagers, en gérant les demandes spéciales, en facilitant les procédures d'embarquement et de débarquement, et en gérant les problèmes liés aux bagages ou aux changements de vol. Les compagnies aériennes utilisent également les données des dossiers passagers à des fins d'analyse pour mieux comprendre les habitudes de voyage des passagers, les tendances du marché et les préférences des voyageurs. Ces

[rgpd-a-une-influence-parce-qu-il-est-et-continuera-a-etre-le-standard-mondial_6174747_4408996.html](#) consulté le 19 juillet 2023.

informations sont précieuses pour adapter les services proposés et améliorer l'expérience globale des passagers.

Lors des réservations, les compagnies aériennes collectent des informations sur les passagers dont le nom, la date du voyage, l'origine, la destination, la date de naissance, l'adresse et le numéro de téléphone, la carte d'identité, le passeport, le moyen de paiement, le numéro de carte de crédit, l'agence de voyages et le numéro de siège. Ces informations, utiles au bon déroulement du voyage, sont complétées par des données privées liées à la personnalisation du voyage comme des préférences alimentaires qui peuvent indiquer les croyances personnelles du voyageur comme ses croyances religieuses. Avec l'adoption de divers actes juridiques sur le PNR, les compagnies sont obligées de transmettre ces informations aux autorités sécuritaires des pays visités. Les informations stockées dans le logiciel de gestion des réservations (Global Distribution Systems – GDS¹⁵⁶²) sont accessibles par un très grand nombre de salariés des agences de voyages. Par ailleurs, les procédures de sécurité entourant ces accès sont insuffisantes. Enfin, le nom du passager et sa référence à six chiffres permettent à n'importe qui d'accéder au dossier sur le site de la compagnie et d'y apporter des modifications ; de plus, ces informations sont présentes dans les courriels et sur les cartes d'embarquement. Il est donc relativement facile de changer le nom du voyageur ou de se faire rembourser son voyage, même si certaines entités ont renforcé leurs procédures de sécurité¹⁵⁶³.

Les durées de stockage, dit aussi conservation, des données des passagers aériens et leur archivage avec anonymisation progressive ont été longuement discutées. Dans le cas de l'accord PNR euro-américain, les durées de quinze ans pour le terrorisme et dix ans pour la criminalité transnationale ont été choisies mais elles semblent excessives pour Xavier Latour¹⁵⁶⁴ malgré la dépersonnalisation des données puisque celle-ci est rétractable. Au-delà de ladite période, les données, bien qu'anonymisées, ne sont pas effacées, rendant la justification de la mesure difficile. Le droit européen fait preuve, quant à lui, de davantage de modération en retenant une période de cinq ans et une dépersonnalisation après six mois,

¹⁵⁶² Global Distribution System (GDS) est un logiciel de gestion des réservations de prestation de voyage dont l'hôtel, le camping ou l'avion, dans le monde pour les voyageurs. Les principaux acteurs sont Amadeus, Sabre et Galileo. Ce logiciel permet à ces voyageurs de connaître les prestations, les disponibilités et leur prix en temps réel.

¹⁵⁶³ AFTM, « Le parcours de la donnée : PNR et voyage des données », Récolte – Législation et protection des données, *Données : de la récolte à la valorisation*, Fiche 14, août 2017, en ligne à URL : https://www.aftm.fr/wp-content/uploads/2017/08/Fiche-14_PNR_et_voyage_des_donnees_LB-AFTM2017.pdf consulté le 16 juillet 2023.

¹⁵⁶⁴ X. LATOUR, « Les fichiers PNR et les transports aériens internationaux », *Annuaire du droit de la sécurité et de la défense*, Mare et Martin, 2018, pp. 247-258.

d'après l'article 12 de la directive PNR. Ces informations permettent aux services de maintien de l'ordre du monde entier d'identifier les terroristes et les criminels dangereux. Pour les défenseurs de la collecte, les données ont permis, par exemple, de prévenir les projets d'attentats terroristes dans le métro de New York en 2009¹⁵⁶⁵.

Les enjeux liés à la conservation des données des passagers aériens sont nombreux et soulèvent des questions importantes en matière de protection juridique. Les politiques et les réglementations entourant la conservation des données PNR varient d'un pays à l'autre. Certains ont mis en place des lois spécifiques régissant l'utilisation et la protection des données des passagers aériens tandis que d'autres ont connu des débats concernant les droits fondamentaux et la proportionnalité de leur utilisation. Une période de conservation adéquate des données des dossiers passagers est nécessaire pour permettre aux autorités compétentes d'effectuer des enquêtes approfondies et d'analyser les informations pertinentes. Si les données sont conservées pendant une durée trop courte, cela pourrait limiter la capacité des autorités à détecter des schémas de voyage suspects ou à les relier des activités criminelles.

La durée de conservation des données PNR est étroitement liée à la protection de la vie privée des passagers. Des périodes de conservation excessivement longues peuvent entraîner une collecte excessive de données et une violation de la vie privée des individus. Il est essentiel de trouver un équilibre entre les besoins légitimes en matière de sécurité et de lutte contre les infractions terroristes ainsi que la criminalité transnationale et la préservation des droits à la vie privée et à la protection des données personnelles. La durée de conservation des données PNR doit être proportionnelle à l'objectif poursuivi. Les autorités doivent justifier une conservation prolongée en démontrant que cela est strictement nécessaire pour atteindre les objectifs de sécurité et de lutte contre la criminalité. Une durée de conservation excessive pourrait être considérée comme une atteinte disproportionnée aux droits fondamentaux. En effet, l'enjeu de la durée de conservation des données PNR réside dans la recherche d'un incessant équilibre entre les besoins de sécurité et de lutte contre la criminalité grave, d'une part, et le respect de la vie privée et la protection des données à caractère personnel, d'autre part.

¹⁵⁶⁵ Europa, « Accord entre l'Union européenne et les États-Unis concernant les données des dossiers des passagers aériens », *Eur-Lex*, 26 août 2021.

§ 2 – Des actes juridiques européens encadrant la durée de conservation des données sous la pression des institutions européennes au nom des droits fondamentaux

Les attentats sur le sol américain du 11 septembre 2001 ont eu pour conséquence d'augmenter l'intérêt pour les fichiers des compagnies aériennes produits pour chaque passager ayant réservé un voyage. Ces dossiers passagers sont stockés sur les bases de données de réservation et de contrôle des départs des compagnies aériennes¹⁵⁶⁶. Ils permettent à tous les opérateurs du secteur aérien dont l'agence de voyages, les agents d'assistance en escale, les systèmes informatisés et les transporteurs aériens, de suivre chaque passager et d'avoir accès à toutes les informations pertinentes à propos de son voyage, notamment sur ses vols aller et retour, ses vols de correspondance, le cas échéant, ses services particuliers demandés à bord, etc. La nature et le nombre des champs d'information dans un système PNR varient d'une compagnie aérienne à l'autre et d'un passager à l'autre. Un système PNR peut compter jusqu'à une soixantaine de champs et sous-champs¹⁵⁶⁷. La conservation des données des dossiers passagers a très tôt fait l'objet d'âpres débats. Déjà en 2007, la Commission avait soumis le projet de proposition de décision-cadre¹⁵⁶⁸ du Conseil relative à l'utilisation des données des dossiers passagers au Contrôleur européen de la protection des données pour avis. La proposition portait sur le traitement des données des dossiers passager au sein de l'Union européenne et était étroitement liée à d'autres mécanismes de collecte et d'utilisation des données relatives aux passagers, en particulier l'accord intervenu entre Européens et les Américains en juillet 2007.

Ces mécanismes juridiques intéressaient vivement le CEPD¹⁵⁶⁹, qui avait déjà eu l'occasion de formuler des observations sur le questionnaire¹⁵⁷⁰ de la Commission relatif au système PNR prévu par l'Union européenne, soumis en décembre 2006 aux parties intéressées, les États membres, les autorités de protection des données et les associations de transporteurs aériens. Ce questionnaire avait été établi en vue de l'élaboration d'une analyse d'impact de la

¹⁵⁶⁶ S. RODRIGUES, « Transports aériens », *Répertoire de droit européen*, Dalloz, 2018.

¹⁵⁶⁷ MEMO/07/294 du 13 juillet 2007 de la Commission européenne.

¹⁵⁶⁸ Commission européenne, Proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives, COM(2007) 654 final, 6 novembre 2007.

¹⁵⁶⁹ CEPD, Avis sur le projet de proposition de décision cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record — PNR) à des fins répressives, 1^{er} mai 2008.

¹⁵⁷⁰ CEPD, Avis sur le questionnaire de la Commission relatif au système PNR prévu par l'Union européenne, décembre 2006.

proposition par la Commission européenne de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers¹⁵⁷¹.

Dans ce contexte, le CEPD avait rendu un avis, le 1^{er} mai 2008, sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers à des fins répressives. Le CEPD nota que l'article 9 de la proposition prévoyait une période de conservation des données PNR d'une durée de cinq ans avec une période supplémentaire de huit années « durant laquelle les données doivent être conservées dans une base de données passive, qui sera accessible dans des conditions limitées »¹⁵⁷². Le CEPD avait émis des doutes « quant à la différence établie entre les deux types de bases de données » puisque rien ne garantissait que la base de données passive puisse constituer « un véritable système d'archivage, avec des méthodes distinctes de conservation et d'extraction des données »¹⁵⁷³. Cette réticence s'expliquait par le fait que la majorité des conditions fixées pour « accéder à la base de données passive sont des exigences de sécurité qui pourraient tout aussi bien s'appliquer à la base de données utilisée pour conserver les données pendant cinq ans »¹⁵⁷⁴.

Par ailleurs, la durée totale de conservation, de treize ans, a été jugée excessive, car même si elle était justifiée dans l'analyse d'impact par la nécessité de mettre en place des indicateurs de risques et d'élaborer des modèles de déplacement et de comportement, son efficacité restait à démontrer pour le CEPD. Pour ce dernier, « s'il est évident que les données peuvent être conservées aussi longtemps que nécessaire dans un cas particulier et dans la mesure où une enquête est en cours », rien ne permettait de justifier une durée de conservation aussi longue vis-à-vis de tous les passagers « lorsqu'aucun soupçon ne pèse sur eux »¹⁵⁷⁵.

Le CEPD a en outre noté que cette période de conservation n'était pas étayée par les réponses des États membres au questionnaire de la Commission selon lesquelles la période de conservation moyenne requise était de trois ans et demi. De plus, les critiques ont remarqué que cette période de treize ans était comparable à la période de conservation de quinze ans prévue dans le plus récent accord PNR avec les États-Unis. Le CEPD avait toujours soutenu qu'une période de conservation aussi longue n'avait été adoptée qu'en raison d'une forte pression du Gouvernement américain pour la conserver pendant une période supérieure à trois ans et demi, et non parce qu'elle avait été à tout moment défendue par le Conseil ou la

¹⁵⁷¹ CEPD, « Avis du Contrôleur européen de la protection des données du 1^{er} mai 2008 sur le projet de proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives », JOUE n° C 110, 1^{er} mai 2008.

¹⁵⁷² Ibidem.

¹⁵⁷³ Ibidem.

¹⁵⁷⁴ Ibid.

¹⁵⁷⁵ Ibid.

Commission. Le CEPD a ainsi considéré qu'il n'y avait aucune raison d'introduire un tel compromis dans un instrument juridique adopté par l'Union européenne dans l'unique but de faire aboutir des négociations jugées difficiles mais inévitables¹⁵⁷⁶.

Cet avis du CEPD est important en matière de conservation des données à caractère personnel des passagers aériens pour plusieurs raisons. Tout d'abord, comme organe consultatif indépendant de l'Union européenne chargé de veiller à ce que la législation européenne en matière de protection des données soit respectée. Son rôle est de protéger les droits fondamentaux des individus en matière de vie privée et de protection des données à caractère personnel. Par conséquent, cet avis a pu jouer un rôle essentiel pour garantir que la conservation des données respecte les principes et les normes établis dans le cadre de la législation européenne sur la protection des données. Lorsque des entreprises ou des organisations souhaitent conserver des données à caractère personnel, elles doivent se conformer aux obligations légales en matière de protection des données telles que la nécessité d'obtenir le consentement des personnes concernées, de limiter la collecte et la conservation des données au strict nécessaire, de garantir la sécurité des données, et de respecter les droits des individus (accès, rectification, suppression, etc.). Le CEPD joue un rôle crucial dans l'évaluation de la conformité des pratiques de conservation des données avec ces exigences légales.

Ensuite, cet avis est intéressant, car il peut contribuer à garantir une application uniforme et cohérente des règles de protection des données dans toute l'Union européenne. Le CEPD¹⁵⁷⁷ fournit des orientations et des recommandations aux autorités de contrôle nationales chargées de superviser la protection des données dans chaque État membre. Cela contribue à éviter des interprétations divergentes de la loi et à garantir une approche harmonisée de la conservation des données à caractère personnel.

Enfin, cet avis du CEPD a pu avoir un poids considérable dans le processus décisionnel vis-à-vis de la directive PNR : bien que l'avis du CEPD ne soit pas contraignant, il est pris en compte par les institutions européennes et les législateurs lorsqu'ils élaborent de nouvelles réglementations ou politiques liées à la protection des données. Cet avis a pu influencer les décisions prises par les autorités compétentes et renforcer les garanties de protection des données pour les dossiers passagers.

¹⁵⁷⁶ Ibid.

¹⁵⁷⁷ CNIL, « Le Comité européen de la protection des données », 16 juillet 2018, en ligne à URL : <https://www.cnil.fr/fr/le-comite-europeen-de-la-protection-des-donnees-cepd#:~:text=Le%20CEPD%20est%20institu%C3%A9%20par,pays%20membres%20de%20l'UE> consulté le 20 juillet 2023.

En résumé, un avis de ce type est important pour la conservation des données à caractère personnel, car le CEPD veille à la conformité avec la législation européenne sur la protection des données, favorise l'harmonisation des pratiques et apporte une expertise indépendante qui renforce la protection des droits fondamentaux des individus en matière de vie privée et de protection des données. En effet, l'utilisation des données des dossiers passagers a toujours été un sujet délicat en matière de protection des données à caractère personnel, car d'une part, ces données peuvent être utilisées pour lutter contre des crimes graves tels que le terrorisme, le trafic de drogue et la traite des êtres humains, en permettant aux autorités compétentes de détecter des modèles de comportement suspects mais d'autre part, cela soulève des questions importantes concernant la protection des droits fondamentaux des individus, dont le droit à la vie privée et à la protection des données. Aujourd'hui, ces données PNR sont conservées cinq ans¹⁵⁷⁸ à compter de leur réception dans le système. À l'expiration d'un délai de deux ans, ces éléments susceptibles de révéler directement l'identité des passagers sont conservés mais ne peuvent plus être transmis aux services demandeurs. La directive du 27 avril 2016 relative à l'utilisation des données des dossiers passagers prévoit cette « dépersonnalisation » des données, c'est-à-dire un masquage de certaines données, à l'expiration d'une période de six mois¹⁵⁷⁹. Ce n'est que sur demande motivée et après autorisation expresse du directeur de l'UIP que les agents habilités peuvent en être destinataires. Les citoyens européens disposent d'un droit d'accès et de rectification. En France, pour les données des dossiers passagers, les droits d'accès et de rectification s'exercent directement auprès du directeur de l'UIP ou de son adjoint¹⁵⁸⁰, basés à l'aéroport de Roissy-Charles de Gaulle.

¹⁵⁷⁸ Directive PNR, article 12, alinéa 1.

¹⁵⁷⁹ Directive PNR, article 12, alinéa 2. Voir en ce sens : CNIL, « Le système API-PNR France », 10 août 2016, en ligne à URL : <https://www.cnil.fr/fr/le-systeme-api-pnr-france> consulté le 20 juillet 2023.

¹⁵⁸⁰ Directive PNR, article 4, 5. Voir également : Décret n° 2018-722 du 3 août 2018 modifiant le décret n° 2014-1566 du 22 décembre 2014 portant création d'un service à compétence nationale dénommé « Unité Information Passagers » (UIP).

Chapitre 2 – Une déterritorialisation limitée par l’implication des États dans les crises contemporaines : le retour du droit national dans l’utilisation des données personnelles

L’État est généralement associé à un gouvernement qui exerce de manière souveraine la totalité de ses compétences sur un territoire aux frontières clairement tracées. Historiquement, avec l’avènement de la modernité¹⁵⁸¹, la « territorialisation » du pouvoir politique s’est développée parallèlement à la priorité accordée à la protection de la souveraineté territoriale. Mais depuis plusieurs années, les chercheurs en politique comme les sociologues ont mis en avant un phénomène de « déterritorialisation » du pouvoir politique, entendu comme l’un des aspects de l’avènement de l’époque postmoderne¹⁵⁸². Du fait à la fois de la montée en puissance des organisations internationales et de l’hégémonie ascendante des acteurs privés, l’État dispose de moins en moins de pouvoirs sur son territoire.

Le professeur Jacqueline Morand Deviller souligne que la notion de territoire, initialement valorisée par les géographes, a été intégrée par les juristes en droit international public, devenant l’une des trois composantes fondamentales de l’État. Ce dernier exerce, dans son territoire, pleinement et exclusivement ses compétences, parmi lesquelles la garantie de la sécurité. Cela donne naissance au concept de « territoire limite », qui permet à l’État de définir la sécurité dans un espace clairement délimité¹⁵⁸³. Cependant, tout comme l’abus de langage, l’abus des découpages territoriaux tend à dénaturer ce concept, creusant le décalage entre le support verbal et la réalité qui lui est associée. Morand Deviller convoque le terme de « territoire fiction » dans un contexte où les frontières deviennent modulables et le territoire, sans limites¹⁵⁸⁴. Ce flou dans les termes et concepts entraîne une perte de lisibilité et de portée, rendant difficile la compréhension des véritables enjeux juridiques et administratifs liés à cette notion.

Conséquemment, les frontières voient leur sens radicalement modifié ; alors qu’elles constituaient autrefois des lignes précises et définies délimitant la séparation radicale des

¹⁵⁸¹ C. RAFFESTIN, & M. BRESSO, « Tradition, modernité, territorialité », *Cahiers de géographie du Québec*, 1982, en ligne à URL : <https://doi.org/10.7202/021557ar> consulté le 20 juillet 2023.

¹⁵⁸² O. CORTEN, « Vers une « déterritorialisation » de l’interdiction du recours à la force dans les relations internationales ? », *Organization of American States*, 7 juillet 2010, en ligne à URL : http://www.oas.org/dil/esp/XXXVII_Curso_vers_une_Leonardo_Nemer.pdf consulté le 20 juillet 2023.

¹⁵⁸³ J. MORAND-DEVILLER, « Le territoire fiction », *Actualité juridique droit administratif*, Dalloz, 2000, p.1461.

¹⁵⁸⁴ Ibidem.

pouvoirs étatiques voisins ou concurrents, elles tendent progressivement à se réduire à de simples symboles et l'exercice du pouvoir extraterritorial se développe parallèlement aux phénomènes d'intégration régionale. Dans son essai *La fin des territoires*¹⁵⁸⁵ publié en 1995, Bertrand Badie avait déjà analysé les transformations dans les relations internationales à l'ère de la mondialisation, mettant l'accent sur les changements et les défis profonds auxquels les traditionnels États-nations et les territoires sont plus en plus confrontés dans un monde toujours plus interconnecté. Pour le chercheur français, la mondialisation a conduit à l'affaiblissement de la souveraineté traditionnelle des États-nations. Conséquemment, les frontières cloisonnent de moins en moins dans un monde de flux importants de personnes, de capitaux, de biens et d'informations qui transcendent les limites nationales.

Par ailleurs, la mondialisation a favorisé la montée en puissance d'acteurs non-étatiques tels que les organisations non gouvernementales (ONG), les mouvements sociaux transnationaux, les entreprises multinationales, dont les acteurs du monde aérien. Ces acteurs jouent un rôle croissant dans les affaires mondiales, comme le montrent les compagnies aériennes comme Qatar Airways¹⁵⁸⁶ en défiant le monopole traditionnel de l'État dans les relations internationales.

De manière plus grave, le politologue met l'accent sur l'émergence d'une politique mondiale qui transcende les frontières nationales. Les enjeux mondiaux tels que le terrorisme, la criminalité grave, les changements climatiques, les migrations et les pandémies nécessitent une coopération et une action collective à l'échelle mondiale, que l'État n'est plus capable de gérer seul. L'interdépendance croissante des nations remet en question la capacité des États à agir de manière autonome et à répondre efficacement aux problèmes mondiaux ; ils sont confrontés à de nouveaux défis qui peuvent parfois remettre en cause leur autorité et leur légitimité.

La crise mondiale du Covid-19 a entraîné des questionnements sur l'avenir de l'ordre mondial tel qu'il existe depuis 1945. En effet, cette pandémie a entraîné plusieurs conséquences sur les économies mondiales. Tout d'abord, les restrictions de confinement, les fermetures d'entreprises et les perturbations des chaînes d'approvisionnement ont entraîné une contraction économique majeure dans de nombreux pays, entraînant des récessions économiques. Certains secteurs ont été durement touchés par la pandémie tandis que d'autres ont prospéré.

¹⁵⁸⁵ B. BADIE, *La fin des territoires*, Fayard, Paris, 1995.

¹⁵⁸⁶ A. AUTIN, « Voici la meilleure compagnie aérienne du monde en business class (ce n'est pas Air France ni Singapour Airlines) », *GQ Magazine*, 13 décembre 2023, en ligne à URL : <https://www.gqmagazine.fr/article/meilleure-compagnie-aerienne-du-monde-en-business-class-qatar-airways-et-pas-air-france-ni-singapour-airlines> consulté le 21 janvier 2024.

Par exemple, les entreprises technologiques et de livraison en ligne ont vu leur activité augmenter alors que les industries liées au tourisme et à l'hôtellerie ont souffert.

Dans son essai *Les capitalismes à l'épreuve de la pandémie*¹⁵⁸⁷, Robert Boyer donne à comprendre les processus déclenchés en 2020 et éclaire sur la fragmentation des relations internationales, la fragilisation de la zone euro, la déstabilisation de l'État social et la montée des populismes. Les personnes vulnérables dans le système économique capitaliste se sont tournées vers l'État, vu comme protecteur, car il est apparu le seul capable de les protéger de la misère et du déclassement face à la « toute-puissance des firmes transnationales du numérique et de la finance – mais aussi réhabilités dans leurs fonctions régaliennes et régulatrices par la "magie" de la pandémie. La puissance des GAFA produit donc sa contrepartie dialectique : la poussée de différents capitalismes d'État prêts à défendre leurs prérogatives – et leurs propres entreprises – derrière leurs frontières, dont le modèle le plus achevé est la Chine »¹⁵⁸⁸. La Chine reste tout de même un exemple particulier au regard des mesures maximalistes qu'elle a pu prendre. En Europe, le Royaume-Uni a pris des mesures assez strictes¹⁵⁸⁹. Pour atténuer les effets négatifs de la pandémie, de nombreux gouvernements ont mis en place des mesures d'aide économique telles que des subventions aux entreprises, des prestations de chômage et des programmes d'aide sociale. Cela a entraîné une augmentation de l'intervention étatique dans l'économie.

Dans ce contexte, le processus de déterritorialisation¹⁵⁹⁰ observé, à savoir celui dans lequel les activités, les relations sociales et les influences dépassent les frontières traditionnelles des territoires nationaux et deviennent plus transnationales ou globales, est à nuancer. Avec la multiplication des crises, phénomène que l'on nomme aujourd'hui « polycrise »¹⁵⁹¹, on observe un retour de l'État comme une réponse aux défis posés par la déterritorialisation. Ainsi, la reterritorialisation intervient comme un phénomène dans lequel certains acteurs politiques ou institutions vont chercher à renforcer leur contrôle et leur influence dans des territoires spécifiques, comme une réponse aux défis économiques, politiques ou sociaux liés à la mondialisation et à la déterritorialisation.

¹⁵⁸⁷ R. BOYER, *Les capitalismes à l'épreuve de la pandémie*, La Découverte, 2021.

¹⁵⁸⁸ A. REVERCHON, « Robert Boyer : 'Le capitalisme sort considérablement renforcé par cette pandémie' », *Economie française*, *Le Monde*, 2 octobre 2020, en ligne à URL : https://www.lemonde.fr/idees/article/2020/10/02/robert-boyer-le-capitalisme-sort-considerablement-renforce-par-cette-pandemie_6054441_3232.html consulté le 21 juillet 2023.

¹⁵⁸⁹ R. McMASTER, « La pandémie de Covid-19 en Écosse et au Royaume-Uni, entre "déficits" de soins et solidarité », *Revue française de socio-économie*, 2021/1, n° 26, 2021.

¹⁵⁹⁰ H. THERY, « Mondialisation, déterritorialisation, reterritorialisation », *Bulletin de l'Association de Géographes Français*, vol. 85-3, 2008, pp. 324-331.

¹⁵⁹¹ J.-M. POTTIER, « Polycrise », *Sciences humaines*, Actualité de la recherche, mensuel n° 358, mai 2023.

Dans le champ de la protection des données à caractère personnel des passagers aériens, notamment depuis la crise du Covid-19, on peut observer un processus par lequel les acteurs gouvernementaux vont chercher à renforcer leur pouvoir et leur contrôle dans la maîtrise des flux de passagers aériens pour répondre aux défis de la pandémie en investissant notamment dans le contrôle et les technologies aux frontières nationales en vue d'une meilleure maîtrise de l'espace géographique, dont les plateformes aéroportuaires.

Ainsi, au début de la pandémie, les autorités de transport chinoises ont utilisé des caméras thermiques pour détecter les passagers qui présentaient une température anormale. En Chine, tout un réseau national¹⁵⁹² est mis en place pour tracer les individus, grâce à l'identifiant lié à un numéro de portable, avec l'appui des opérateurs mobiles et des autorités publiques pour appliquer ce système de surveillance. Par ailleurs, des start-ups travaillent à produire des logiciels capables de traiter ce big data au profit de l'État chinois¹⁵⁹³.

Cette crise sanitaire a offert un prétexte certains gouvernements pour justifier un pillage massif des données de leurs citoyens au nom de la protection de la collectivité et de lutte contre la pandémie. Il n'y avait alors que très peu de considérations pour la protection des données à caractère personnel. On assiste donc à un retour de l'État dans un domaine dans lequel il tendait auparavant à laisser de plus en plus de place aux opérateurs privés.

Section 1 – Vers une probable extension par les États du champ d'application des dossiers passagers à la santé : une conséquence de la crise du coronavirus

Dans le contexte de la crise sanitaire liée au coronavirus, les entreprises comme les entités publiques ont été amenées à discuter des mesures à prendre pour limiter la propagation du virus et des conditions de protection des données à caractère personnel ; il a notamment été question de la possibilité de collecter des données sur des employés ou des agents en dehors de la prise en charge médicale, pour déterminer si ces personnes présentaient des symptômes du coronavirus, ou des données liées à des déplacements et des activités pouvant relever de la sphère privée. La CNIL a considéré que chaque entité devait prendre des mesures adaptées à la situation, comme limiter les déplacements et les réunions ainsi que respecter les mesures

¹⁵⁹² L. ASGARALI, « L'arsenal technologique de la Chine pour lutter contre le coronavirus », *Le Figaro*, Tech & web, 17 février 2020, en ligne à URL : <https://www.lefigaro.fr/secteur/high-tech/detecteur-de-chaleur-corporelle-drones-la-chine-recourt-massivement-aux-technologies-pour-contenir-le-coronavirus-20200207> consulté le 20 juillet 2023.

¹⁵⁹³ 20 Minutes, « Coronavirus : La Chine utilise des lunettes connectées pour détecter les personnes à risque », *Le Monde*, High-Tech, 27 mars 2020, en ligne à URL : <https://www.20minutes.fr/monde/2749611-20200327-coronavirus-chine-utilise-lunettes-connectees-detecter-personnes-risque> consulté le 21 juillet 2023.

d'hygiène¹⁵⁹⁴. Aussi, les employeurs ne pouvaient prendre des mesures susceptibles de porter atteinte au respect de la vie privée des personnes concernées, notamment la collecte de données de santé au-delà de la gestion des suspicions d'infections.

D'autres mesures ont suscité des polémiques dans le débat public comme la mise en place d'un pass sanitaire, notamment avec des applications mobiles qui enregistraient et conservaient des données à caractère personnel, surtout des données sensibles, car elles contenaient des données relevant de la santé de la personne concernée.

La CNIL a été consultée à plusieurs reprises concernant les projets d'applications mobiles impliquant le traitement des données personnelles des citoyens français¹⁵⁹⁵. Elle a notamment examiné les aspects techniques de ces dispositifs pour s'assurer qu'ils respectent les droits à la protection des données personnelles et à la vie privée. Dans ce cadre, la CNIL a formulé des recommandations spécifiques visant à renforcer les garanties en matière de sécurité et de confidentialité des données traitées par ces applications¹⁵⁹⁶.

La CNIL valida ces applications tout en posant des conditions qui devaient garantir la non-transmission des données à d'autres serveurs et la protection des informations liées au statut vaccinal de la personne concernée. Les fournisseurs des applications devaient ainsi être en mesure de garantir à l'utilisateur le respect de règles minimum de sécurité, compte tenu des risques d'atteinte à la protection des données personnelles et à la vie privée.

La pandémie du coronavirus s'est déclenchée alors que le RGPD¹⁵⁹⁷ était déjà en vigueur et cette législation européenne a dû être respectée par l'ensemble des États de l'Union européenne. De plus, le RGPD comprend des dispositions permettant l'activation d'exceptions spécifiques dans des circonstances exceptionnelles comme une pandémie, pour protéger la santé publique et les intérêts vitaux¹⁵⁹⁸. Les États membres de l'Union européenne devaient ainsi mettre en place des règles et des mesures spécifiques pour gérer la crise, ce qui signifia que la mise en œuvre exacte des principes du RGPD pouvait varier d'un pays à l'autre

¹⁵⁹⁴ Lamyline, « Coronavirus (Covid-19) : les rappels de la CNIL sur la collecte de données personnelles », *Revue Lamy Droit de l'immatériel*, n° 169, 1^{er} avril 2020.

¹⁵⁹⁵ CNIL, délibération n° 2021-004 du 14 janvier 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19.

¹⁵⁹⁶ CNIL, délibération n° 2021-139 du 21 octobre 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 (mai à septembre 2021). Voir en ce sens : CNIL, « La CNIL précise les garanties que doit respecter la fonctionnalité TousAntiCovid-Carnet », *Dossier Covid-19*, 22 avril 2021, en ligne à URL : <https://www.cnil.fr/fr/la-cnil-precise-les-garanties-que-doit-respecter-la-fonctionnalite-tousanticovid-carnet> consulté le 23 juillet 2023.

¹⁵⁹⁷ CNIL, « Quelles formalités pour les traitements de données de santé à caractère personnel ? », 8 janvier 2018, en ligne à URL : <https://www.cnil.fr/fr/applications-mobiles-en-sante-et-protection-des-donnees-personnelles-les-questions-se-poser> consulté le 23 juillet 2023.

¹⁵⁹⁸ RGPD, article 9.

bien que l'objectif principal fût de trouver un équilibre entre la protection des données à caractère personnel et la nécessité de lutter contre la propagation de la pandémie de manière efficace.

Toutefois, pendant la crise du Covid-19, de nombreux États ont agi de manière unilatérale en prenant des mesures indépendantes, sans forcément se coordonner avec leurs partenaires pour lutter contre la pandémie. Ce fut le cas des États-Unis d'Amérique¹⁵⁹⁹. La pandémie a touché presque tous les pays du monde et chaque État a dû réagir rapidement et adopter des politiques spécifiques en fonction de sa situation, de sa capacité de réponse et de ses besoins locaux. Durant cette crise, la place de l'État dans la gestion de la pandémie est devenue centrale¹⁶⁰⁰, car celui-ci devait protéger le « bien suprême »¹⁶⁰¹, à savoir la vie humaine et ce « quoiqu'il en coûte »¹⁶⁰² sur le plan des libertés publiques et des dépenses économiques.

Si certains États ont adopté des mesures unilatérales pour faire face à la pandémie, de nombreux pays ont toutefois cherché à coordonner leurs politiques et à travailler ensemble au niveau international pour partager des informations, des ressources et des bonnes pratiques dans la lutte contre la pandémie. La nature mondiale de la crise du Covid-19 a cependant mis en évidence les limites de la coopération internationale et de la coordination entre les États pour relever ces types de défis posés par une pandémie.

Sous-section 1 – La crise du coronavirus, des solutions mettant en danger les données à caractère personnel des passagers aériens

La crise sanitaire s'est accompagnée d'une augmentation du recours à de nouvelles technologies, comme les caméras thermiques, ainsi que des collectes de données, notamment des données de santé, afin de limiter la propagation de la pandémie. Ces mesures ont eu un impact sur le secteur aérien, notamment sur les données à caractère personnel des passagers aériens. On a ainsi assisté à un retour de l'État dans un domaine dans lequel on attendait à ce qu'il continue de laisser de plus en plus de place aux opérateurs privés. En France, à

¹⁵⁹⁹ M.-C. NAVES, « Entre unilatéralisme et dénégation, la gestion de la crise du Covid-19 selon Donald Trump », *IRIS*, 17 avril 2020, en ligne à URL : <https://www.iris-france.org/146292-entre-unilateralisme-et-denegation-la-gestion-de-la-crise-du-covid-19-selon-donald-trump/> consulté le 23 juillet 2023.

¹⁶⁰⁰ R. GAY, K. GUILLAS-CAVAN, « La gestion sanitaire de l'épidémie de Covid-19 par les États : recettes communes et logiques nationales », *Chronique internationale de l'IREs*, 2020/3, n° 171, 2020, en ligne à URL : <https://www.cairn.info/revue-chronique-internationale-de-l-ires-2020-3-page-3.htm&wt.src=pdf> consulté le 23 juillet 2023.

¹⁶⁰¹ F. PIERRU, « Introduction. L'administration hospitalière, entre pandémie virale et épidémie de réformes », *Revue française d'administration publique*, vol. 174, n° 2, 2020, pp. 301-315, en ligne à URL : <https://doi.org/10.3917/rfap.174.0005> consulté le 23 juillet 2023.

¹⁶⁰² E. MACRON, « La France unie, c'est notre meilleur atout dans la période troublée par le Covid-19 que nous traversons. Nous tiendrons. Tous ensemble », Adresse aux Français, *Élysée*, 12 mars 2020, en ligne à URL : <https://www.elysee.fr/emmanuel-macron/2020/03/12/adresse-aux-francais> consulté le 23 juillet 2023.

l'aéroport Roissy-Charles de Gaulle, on a assisté durant la pandémie à un renforcement des forces de sécurité comme la police et les autorités sanitaires présentes pour demander des informations personnelles aux voyageurs en fonction du pays d'où ils venaient, notamment sur la propagation du virus dans ce territoire.

§ 1 – Le monde du droit en adaptation face à une pandémie bouleversant les relations internationales

La pandémie¹⁶⁰³ causée par le virus Covid-19 a touché presque tous les pays du monde. Chaque État a dû réagir rapidement en mettant en place des mesures spécifiques en fonction de sa situation, de sa capacité de réponse et de ses besoins locaux. La pandémie a affecté les différentes formes de capitalisme à travers le monde¹⁶⁰⁴ en posant des défis aux systèmes économiques. Des stratégies d'adaptation ont été mises en œuvre par les acteurs économiques et les gouvernements dans un esprit d'improvisation.

Plusieurs pays ont fermé leurs frontières aux voyageurs en provenance de certains pays particulièrement touchés par le virus, sans forcément coordonner ces décisions avec d'autres pays. Par ailleurs, la quasi-majorité des États du monde ont décidé de mettre en place des mesures de confinement, de fermer des commerces et d'instaurer des quarantaines pour les voyageurs en ne coordonnant pas toujours ces actions avec d'autres pays. Les pouvoirs publics ont fermé écoles, universités et lieux publics sans nécessairement suivre les mêmes calendriers ou les mêmes directives que d'autres nations¹⁶⁰⁵. Certains États ont pris des mesures pour acheter massivement des fournitures médicales comme des masques, des équipements de protection individuelle et des médicaments, sans nécessairement coopérer avec d'autres pays pour assurer une distribution équitable¹⁶⁰⁶.

Par ailleurs, plusieurs nations ont investi massivement dans la recherche et le développement de vaccins et de traitements du Covid-19, en lançant leurs propres programmes nationaux sans nécessairement coopérer avec d'autres pays dans ces efforts. La pandémie a posé un double

¹⁶⁰³ AMELI, « Épidémie, pandémie, gestion sanitaire : ce qu'il faut savoir », *Santé*, 21 juin 2023, en ligne à URL : <https://www.ameli.fr/assure/sante/themes/epidemie-et-pandemie/epidemie-et-pandemie-quelle-difference#:~:text=C'est%20le%20cas%20par,est%20d%C3%A9finie%20comme%20une%20pand%C3%A9mie%20consulté le 24 juillet 2023.>

¹⁶⁰⁴ R. BOYER, *Les capitalismes à l'épreuve de la pandémie*, La Découverte, 2021.

¹⁶⁰⁵ Le Monde, « Coronavirus : Édouard Philippe annonce la fermeture de tous les lieux publics 'non indispensables' », *Politique, Coronavirus et Pandémie de Covid-19*, 14 mars 2020, en ligne à URL : https://www.lemonde.fr/politique/article/2020/03/14/edouard-philippe-annonce-la-fermeture-de-tous-les-lieux-publics-non-indispensables_6033110_823448.html consulté le 24 juillet 2023.

¹⁶⁰⁶ Le Monde, « Pauvreté et crise du multilatéralisme, comment le Covid-19 aggrave les fractures mondiales », *Débats, Coronavirus et pandémie de Covid-19*, 9 avril 2021, en ligne à URL : https://www.lemonde.fr/idees/article/2021/04/09/pauvrete-et-crise-du-multilateralisme-comment-le-covid-19-aggrave-les-fractures-mondiales_6076110_3232.html consulté le 24 juillet 2023.

défi pour les gouvernements et l'industrie pharmaceutique dans la mesure où, d'une part, de nouveaux vaccins devaient être développés pour faire face à cette menace exceptionnelle et, d'autre part, des milliards de doses devaient être produites en très peu de temps¹⁶⁰⁷. Une coopération entre ces différents secteurs a permis d'atteindre ces objectifs. Les premiers vaccins ont été produits en moins de 12 mois alors que cela prend généralement une décennie ou plus. Au 3 février 2021, il y avait 289 vaccins expérimentaux contre le Covid-19 en cours de développement, dont 20 étaient en phase 3 d'essais cliniques. En mars 2021, moins d'un an après que l'épidémie a frappé les pays européens, plus de 34 millions de doses avaient été administrées dans cet espace européen et ce nombre a augmenté rapidement au cours des semaines suivantes¹⁶⁰⁸. Ainsi, 74 millions de doses ont été administrées dans l'Union européenne début avril 2021 et plus de 844 millions de doses avaient été administrées un an plus tard.

La nature mondiale de la crise a mis en évidence l'importance de la coopération internationale et de la coordination entre les États pour relever les défis posés par la pandémie, pourtant le premier réflexe a été unilatéral dans la plupart des nations. Toutefois, il est essentiel de noter que de nombreux pays ont également cherché à coordonner leurs actions et à travailler ensemble au niveau international pour partager des informations, des ressources et des bonnes pratiques dans la lutte contre la pandémie, notamment sous l'impulsion de l'Organisation mondiale de la santé (ci-après OMS)¹⁶⁰⁹.

De plus, avec la crise du Covid-19, les pays à bas revenus¹⁶¹⁰ ont souffert une crise économique sans obtenir d'aide ou de protection, car contrairement aux pays développés ou émergents, ils ne pouvaient ni compter sur des plans généraux de relance, ni sur la dette publique pour résister face au choc créé par la pandémie et encore moins sur une coopération internationale alors que le sort d'un milliard de citoyens était en jeu.

D'après les estimations communiquées, en 2020, par le Conférence des Nations unies sur le commerce et le développement (CNUCED), les 47 États les plus pauvres de la planète ont

¹⁶⁰⁷ M. FLORIO, S. GAMBA, C. PANCOTTI, « Panorama des investissements publics et privés de long terme dans la mise au point de vaccins contre la Covid-19 », *Parlement européen*, Département thématique des politiques économiques, scientifiques et de la qualité de la vie, Etudes, mars 2023, en ligne à URL : [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740072/IPOL_STU\(2023\)740072\(SUM01\)_FR.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740072/IPOL_STU(2023)740072(SUM01)_FR.pdf) consulté le 24 juillet 2023.

¹⁶⁰⁸ Ibidem

¹⁶⁰⁹ OMS, « Stratégie Covid-19 », 14 avril 2020, en ligne à URL : https://www.who.int/docs/default-source/coronaviruse/strategy-update-french.pdf?sfvrsn=b1cfe48a_2 consulté le 24 juillet 2023.

¹⁶¹⁰ J. BOUISSOU, « La pandémie de Covid-19 accroît l'extrême pauvreté dans les pays les plus fragiles », *Le Monde*, 3 décembre 2020, en ligne à URL : https://www.lemonde.fr/economie/article/2020/12/03/la-pandemie-de-covid-19-accroit-l-extreme-pauvrete-dans-les-pays-les-plus-fragiles_6062005_3234.html consulté le 24 juillet 2023.

connu la pire performance de ces trente dernières années avec une contraction de leur produit intérieur brut (PIB) d'environ 0,4 % en moyenne¹⁶¹¹. De nombreux pays pauvres disposaient déjà de systèmes de santé fragile et sous-financés avant la pandémie, les rendant les moins bien préparés pour faire face à une crise sanitaire d'une ampleur mondiale. La multiplication de cas de Covid-19 a mis une énorme pression sur leurs infrastructures médicales, les débordant et les plaçant dans une situation d'incapacité face au besoin de la population. Le 1^{er} décembre 2020 les Nations unies (ONU), à travers leur bureau pour la coordination des affaires humanitaires¹⁶¹², tiraient la sonnette d'alarme face à une crise économique qui se transformait en tragédie humanitaire, lançant un appel humanitaire record de 29 milliards d'euros pour l'année 2021¹⁶¹³.

Cette tragédie que les organisations internationales craignaient s'est confirmée puisqu'en 2021, l'ONU estimait que 274 millions d'individus dans le monde avaient besoin d'aide d'urgence pour l'année 2022, car la crise sanitaire s'ajoutait en fait à d'autres problèmes comme les conflits politiques et les crises écologiques. En décembre 2021, l'ONU aspirait à une aide de 41 milliards de dollars pour 2022 pour venir en aide à 183 millions de personnes parmi les plus vulnérables tout en s'alarmant du fait qu'une personne sur 29 dans le monde avait besoin d'une aide d'urgence¹⁶¹⁴. En effet, les restrictions imposées par les gouvernements pour contenir la propagation de l'épidémie, telles que les fermetures d'entreprises et les confinements, ont entraîné des conséquences désastreuses sur les économies des pays pauvres. Subséquemment, de nombreux travailleurs¹⁶¹⁵, notamment des secteurs informels, ont perdu leurs emplois et leurs moyens de subsistance, ce qui a exacerbé la faim, le chômage¹⁶¹⁶ et la pauvreté dans plusieurs régions du monde. Certains pays pauvres ont également été confrontés à des défis supplémentaires, car de nombreuses personnes souffraient déjà de maladies préexistantes telles que le VIH, la tuberculose et le paludisme¹⁶¹⁷.

¹⁶¹¹ Ibidem

¹⁶¹² ONU, « Global Humanitarian Overview 2020 », OCHA, December 2020.

¹⁶¹³ Ibidem

¹⁶¹⁴ Le Monde, « L'ONU estime que 274 millions de personnes dans le monde auront besoin d'une aide d'urgence en 2022 », Planète, Sécuritaire alimentaire, 2 décembre 2021, en ligne à URL : https://www.lemonde.fr/planete/article/2021/12/02/l-onu-estime-que-274-millions-de-personnes-dans-le-monde-aurent-besoin-d-une-aide-d-urgence-en-2022_6104411_3244.html consulté le 24 juillet 2023.

¹⁶¹⁵ G. DELACROIX, S.LANDRIN, « Coronavirus : en Inde, l'impossible confinement des pauvres », *Le Monde*, le 27 mars 2020, en ligne à URL : https://www.lemonde.fr/international/article/2020/03/27/coronavirus-en-inde-l-impossible-confinement-des-pauvres_6034596_3210.html consulté le 24 juillet 2023.

¹⁶¹⁶ J. CAI, « Young and out of a job in China: how Covid-19 is creating an unemployment crisis », *South China Morning Post*, 14 octobre 2022, en ligne à URL : <https://www.scmp.com/news/china/politics/article/3190569/young-and-out-job-china-how-covid-19-creating-unemployment> consulté le 24 juillet 2023.

¹⁶¹⁷ WHO, « La pandémie de COVID-19 perturbe les services de santé dans le monde entier », Communiqué de presse, 12 décembre 2021, en ligne à URL : <https://www.who.int/fr/news/item/12-12-2021-more-than-half-a->

La pandémie a augmenté le fardeau des systèmes de santé qui étaient déjà submergés par la gestion de ces autres maladies.

Par ailleurs, certains pays ont eu du mal à accéder aux vaccins¹⁶¹⁸ en raison de difficultés logistiques, financières ou de distribution, quand ce n'est pas par manque de solidarité. Cela a retardé leur capacité à atteindre l'immunité collective et à limiter la propagation de l'épidémie. L'OMS a admis que « La pandémie de Covid-19 a mis en lumière les nombreuses failles du système mondial visant à protéger les populations contre les pandémies, à savoir : les personnes les plus vulnérables privées de vaccins ; les personnels de santé qui ne disposent pas des équipements nécessaires pour accomplir leur travail permettant de sauver des vies ; et des approches privilégiant les intérêts personnels qui entravent la solidarité mondiale nécessaire pour faire face à une menace mondiale »¹⁶¹⁹. C'est dans ce contexte que l'Assemblée mondiale de la Santé a convenu d'entamer un processus mondial visant à élaborer et à négocier un accord international en vertu du texte fondateur de l'Organisation mondiale de la Santé afin de « renforcer la prévention, la préparation et la riposte face aux pandémies »¹⁶²⁰.

Ce nouvel instrument avait pour objectif de combler les lacunes mises en évidence par la pandémie, à travers des investissements pour instaurer des mécanismes mondiaux de préparation et d'intervention – y compris à l'interface homme-animal – afin de permettre d'anticiper et de prévenir les futures pandémies et y faire face plus efficacement lorsqu'elles surviennent ; prévoir un financement pérenne et prévisible de la préparation et de la riposte aux urgences sanitaires, y compris au moyen de budgets nationaux, pour soutenir les mesures de préparation et contribuer à faire en sorte que le monde soit préparé et puisse réagir à l'émergence d'agents pathogènes dangereux ; mettre en place des mécanismes de

[billion-people-pushed-or-pushed-further-into-extreme-poverty-due-to-health-care-costs](#) consulté le 24 juillet 2023

¹⁶¹⁸ A. GUILLEMOLES, « Covid-19 : les pays pauvres attendent toujours les vaccins Covax », *La Croix*, 2 juillet 2021, en ligne à URL : <https://www.la-croix.com/Economie/Covid-19-pays-pauvres-attendent-toujours-vaccins-Covax-2021-07-02-1201164379> consulté le 24 juillet 2023.

¹⁶¹⁹ OMS, « L'Assemblée mondiale de la Santé convient d'entamer un processus visant à élaborer un accord mondial historique sur la prévention, la préparation et la riposte face aux pandémies », Communiqué de presse, 1^{er} décembre 2021, en ligne à URL : <https://www.who.int/fr/news/item/01-12-2021-world-health-assembly-agrees-to-launch-process-to-develop-historic-global-agreement-on-pandemic-prevention-preparedness-and-response> consulté le 24 juillet 2023.

¹⁶²⁰ Ibidem

gouvernance et de surveillance pour accroître la confiance, assurer la responsabilisation et favoriser la transparence¹⁶²¹.

La crise sanitaire a également entraîné une augmentation des mouvements de population dans certains pays pauvres de nombreux individus ayant cherché à émigrer vers des régions moins touchées par la crise, disposant de meilleures opportunités de travail, ou avec moins de restrictions en matière de déplacement¹⁶²², créant ainsi une fuite de cerveaux et une perte de compétences dans les pays d'origine. Dans certains pays, comme la Chine, la crise sanitaire a permis de justifier davantage de limitations des libertés publiques ainsi que des atteintes contre les droits de l'Homme et la démocratie¹⁶²³.

En mai 2023, soit à peu près trois ans après l'irruption de la pandémie en Asie, l'OMS a considéré que le Covid-19 n'était plus une urgence de santé publique tout en soulignant que le virus n'avait pas disparu¹⁶²⁴. Ce dernier a touché plus de 765 millions de personnes¹⁶²⁵, dont 7 millions en sont morts, dont près d'une personne sur six aux États-Unis. L'organisation internationale rappela que des milliards de doses de vaccins avaient été administrées dans le monde, permettant de faire reculer le nombre de morts dus à la pandémie.

Par ailleurs, Thierry de Montbrial a confirmé que la crise du Covid-19 a précipité l'affaiblissement du multilatéralisme, déjà entamé, alors qu'elle aurait « dû conduire les principaux États de la planète à affronter leurs responsabilités conjointes »¹⁶²⁶. Les États, notamment les grandes puissances du monde, se sont recroquevillés sur eux-mêmes au nom de la souveraineté, rendant les actions de l'Organisation des Nations unies ou de l'Organisation mondiale de la santé inefficace, car elles dépendent de la coopération

¹⁶²¹ OMS, « Accord mondial sur la prévention, la préparation et la riposte face aux pandémies », Q&R, 28 juin 2023, en ligne à URL : <https://www.who.int/fr/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/pandemic-prevention--preparedness-and-response-agreement> consulté le 24 juillet 2023.

¹⁶²² France info, « https://www.francetvinfo.fr/monde/chine/hong-kong/hong-kong-enregistre-une-baisse-record-de-sa-population-apres-une-emigration-massive-des-residents_5305204.html », *France info avec AFP*, 12 août 2022, en ligne à URL : https://www.francetvinfo.fr/monde/chine/hong-kong/hong-kong-enregistre-une-baisse-record-de-sa-population-apres-une-emigration-massive-des-residents_5305204.html consulté le 24 juillet 2023.

¹⁶²³ M.-V. BERNARD, « 'N'importe qui peut être arrêté' : à Hong Kong, la Chine a réduit la société civile au silence », *France info*, 1^{er} juillet 2022, en ligne à URL : https://www.francetvinfo.fr/monde/chine/hong-kong/n-importe-qui-peut-etre-arrete-a-hong-kong-la-chine-a-reduit-la-societe-civile-au-silence_5226565.html consulté le 24 juillet 2023.

¹⁶²⁴ WHO, « Statement on the fifteenth meeting of the IHR (2005) Emergency Committee on the COVID-19 pandemic », *Statement*, 5 mai 2023, en ligne à URL : [https://www.who.int/news/item/05-05-2023-statement-on-the-fifteenth-meeting-of-the-international-health-regulations-\(2005\)-emergency-committee-regarding-the-coronavirus-disease-\(covid-19\)-pandemic](https://www.who.int/news/item/05-05-2023-statement-on-the-fifteenth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic) consulté le 24 juillet 2023.

¹⁶²⁵ Courrier international, « L'OMS met fin à l'urgence de santé publique planétaire pour le Covid-19 », Covid-19, 5 mai 2023, en ligne à URL : <https://www.courrierinternational.com/article/virus-l-oms-met-fin-a-l-urgence-de-sante-publique-planetaire-pour-le-covid-19> consulté le 24 juillet 2023.

¹⁶²⁶ T. DE MONTBRIAL, « Conséquences et leçons d'un virus », *Ifri*, 1^{er} juillet 2020, en ligne à URL : <https://www.ifri.org/fr/publications/editoriaux-de-lifri/consequences-lecons-dun-virus> consulté le 24 juillet 2023.

internationale et des « troupes » qui en découlent, face à la multiplication des crises qui se profilent¹⁶²⁷. Pourtant, la lutte contre une telle pandémie requerrait collecte et interprétation des données, leur partage, une organisation régionale et internationale de prévention face aux risques sanitaires, économiques et politiques, la répartition des responsabilités qui en découlent et la mise en place d'un financement global¹⁶²⁸. La gouvernance a ainsi montré ses limites devant cette pandémie. Or, le droit international, grâce à ses instruments, a pu jouer dans le passé ce rôle d'amortisseur face aux nombreuses crises traversées par les États. Sans coopération internationale, la crise a plongé des millions de personnes dans la pauvreté.

Pour Thierry de Montbrial, cette crise a ainsi ouvert la voie à un « renforcement de la politisation de l'économie internationale, c'est-à-dire à une accentuation de la corrélation entre géopolitique, géostratégie et géoéconomie. Le tout formant une sorte de "géo" à la puissance trois. Les États s'attacheront de plus en plus ouvertement à protéger celles de leurs entreprises qu'ils considéreront comme "stratégiques", ou tout au moins des points jugés critiques de leurs activités. Le droit à la concurrence s'en trouvera bouleversé. (...) Les investissements directs et les mouvements de population seront de plus en plus contrôlés »¹⁶²⁹. Cette évolution est analysée par le politiste comme un « retour partiel » vers une forme « prémoderne » d'une économie internationale dans laquelle les États échangent essentiellement des biens alors que le capital et le travail deviennent peu mobiles¹⁶³⁰.

§ 2 – Une crise sanitaire entraînant des conséquences concrètes sur le traitement des données personnelles

Chaque seconde, les chercheurs, les infirmiers, les pharmaciens, les médecins et les autorités régulatrices produisent et utilisent, partout dans le monde, un grand nombre de données relatives aux domaines de la santé qui sont essentielles à leur travail consistant à préserver la vie des citoyens. Pour l'Union européenne, les données de santé « constituent le sang qui coule dans les veines » des systèmes de soins de santé¹⁶³¹.

Durant la pandémie du Covid-19, les données de santé actualisées ont été jugées cruciales face aux crises et ont permis de prendre des mesures de santé publique avec une meilleure

¹⁶²⁷ Ibidem

¹⁶²⁸ T. DE MONTBRIAL, « Le bien public mondiale, au-delà des mots », *Ifri*, 3 juin 2020, en ligne à URL : <https://www.ifri.org/fr/publications/editoriaux-de-lifri/bien-public-mondial-dela-mots> consulté le 24 juillet 2023.

¹⁶²⁹ T. DE MONTBRIAL, « Après le multilatéralisme, les grandes guerres ? », *Ifri*, 3 août 2020, en ligne à URL : <https://www.ifri.org/fr/espace-media/lifri-medias/apres-multilateralisme-grandes-guerres> consulté le 24 juillet 2023.

¹⁶³⁰ Ibidem

¹⁶³¹ Commission européenne, « Santé dans l'UE : l'espace européen des données de santé (EHDS) », Coin presse, 3 mai 2022, en ligne à URL : https://ec.europa.eu/commission/presscorner/detail/fr/qanda_22_2712 consulté le 25 juillet 2023.

connaissance de la situation. La pandémie a notamment provoqué une forte accélération d'instruments numériques pour lutter contre cette crise sanitaire. Toutefois, des obstacles complexes ont parfois rendu difficile l'exploitation de tout le potentiel du négus des données de santé et du numérique¹⁶³².

S'agissant de l'utilisation primaire de données de santé pour la fourniture de service dans ce domaine, de nombreuses études expliquent que certains États de l'Union européenne ont atteint un niveau élevé de numérisation et d'interopérabilité à l'intérieur de leur territoire tandis que d'autres travaillaient pour prendre les mesures nécessaires. Les dossiers des patients et les services de prescription électronique existent dans les deux tiers des États membres et la plupart sont accessibles via des portails en ligne mais dans quelques pays, ces dossiers et prescriptions peuvent être envoyés ou reçus au-delà des frontières. En outre, onze pays utilisent encore un support papier pour les prescriptions. Aujourd'hui, seulement dix États membres soutiennent le partage des dossiers de patients et des prescriptions électroniques avec l'application de l'Union européenne « MyHealth@EU »¹⁶³³. Toutefois, il est prévu que tous les États membres adoptent ce dispositif numérique d'ici à 2025.

Des études¹⁶³⁴ ont également été réalisées quant à l'utilisation secondaire des données de santé à des fins de recherche, d'innovation, d'élaboration de politiques et de réglementation. Permettant d'éclairer les décisions juridiques, ces études sont aujourd'hui souvent réalisées avec des bases de données rassemblées dans un certain nombre d'États membres. Par conséquent, la taille démographique et géographique de leurs échantillons s'en trouve limitée.

Pour remédier à cette fragmentation et à cette dépendance excessive au consentement, certains États membres ont commencé à adopter des lois nationales¹⁶³⁵. Par exemple, treize États membres ont instauré des systèmes nationaux plus centralisés pour permettre l'accès aux données¹⁶³⁶. Bien que ces systèmes présentent de nombreuses similitudes, ils ne sont pas connectés au niveau européen. Ainsi, ils restent séparés et il existe des différences dans les

¹⁶³² Ibidem

¹⁶³³ MyHealth@EU est une infrastructure numérique transfrontalière pour échanger les données de santé lors de prestations de soins. En ligne à URL : https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_fr consulté le 25 juillet 2023.

¹⁶³⁴ Commission européenne, « Santé dans l'UE : l'espace européen des données de santé (EHDS) », Coin presse, 3 mai 2022, en ligne à URL : https://ec.europa.eu/commission/presscorner/detail/fr/qanda_22_2712 consulté le 25 juillet 2023.

¹⁶³⁵ En France, on peut mentionner la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé qui crée une plateforme ayant pour rôle de réunir, organiser et mettre à disposition les données du système national des données de santé.

¹⁶³⁶ En Allemagne, le centre de recherche « Forschungsdatenzentren » réunit les données de santé qui sont accessibles à des fins scientifiques tout en respectant les règles en matière de protection des données personnelles.

tâches qu'ils accomplissent. Un certain nombre d'États ont mis en place des organismes responsables de l'accès aux données de santé, par exemple l'Allemagne (*Forschungsdatenzentren*), la France (*Health Data Hub*), la Finlande (*Findata*), parmi d'autres¹⁶³⁷.

Le règlement européen, entré en application le 25 mai 2018, renforce la responsabilité des organismes qui traitent ce type de données qui doivent dorénavant assurer une protection optimale des données et être en mesure de documenter leur conformité. Aussi, les personnes dont les données de santé sont collectées disposent de différents droits, dont celui d'être informé¹⁶³⁸. D'après le RGPD, l'information permet aux patients comme aux participants à une recherche de conserver la maîtrise sur leurs données, dans un secteur où agissent différents responsables de traitement comme les professionnels de la santé, les fournisseurs de solutions techniques, les structures de soins, etc.

Cet acte juridique européen a renforcé le droit à l'information des personnes, notamment son contenu, par exemple la durée de conservation et les coordonnées du délégué à la protection des données. Par ailleurs, le règlement prévoit que cette information doit être transparente, concise, compréhensible et aisément accessible. Aussi, les responsables de traitement doivent recenser les différentes mentions et documents d'information et vérifier que ces derniers respectent bien les exigences du règlement sur le fond, à savoir sur le contenu, et sur la forme, notamment la lisibilité¹⁶³⁹. En outre, ce règlement est fondé sur la responsabilisation des acteurs et le rôle donné au consentement des personnes. Cette évolution est justifiée par la maturité plus avancée des responsables de traitement de données de santé vis-à-vis de leurs obligations au regard de la loi.

L'article 4-15 du RGPD définit les données de santé comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de soins de santé, qui révèlent des informations sur l'état de santé de cette personne »¹⁶⁴⁰. Passées, présentes ou futures, ces données incluent les informations relatives à une personne physique, les informations obtenues lors du test ou de l'examen d'une partie du

¹⁶³⁷ Commission européenne, « Santé dans l'UE : l'espace européen des données de santé (EHDS) », Coin presse, 3 mai 2022, en ligne à URL : https://ec.europa.eu/commission/presscorner/detail/fr/qanda_22_2712 consulté le 25 juillet 2023.

¹⁶³⁸ CNIL, « Traitement de données de santé : comment informer les personnes concernées ? », 4 avril 2018, en ligne à URL : <https://www.cnil.fr/fr/traitement-de-donnees-de-sante-comment-informer-les-personnes-concernees> consulté le 25 juillet 2023.

¹⁶³⁹ Ibidem

¹⁶⁴⁰ RGPD, article 4-15.

corps ou les informations concernant une maladie comme les antécédents médicaux ou un handicap¹⁶⁴¹.

L'article 9¹⁶⁴² dudit règlement interdit le traitement de ces données portant sur des catégories particulières de données à caractère personnel, qui peuvent révéler des informations liées à l'appartenance syndicale ou les opinions politiques. Les données de santé en font partie, ce qui rend leur traitement interdit en principe. Le législateur européen entend par traitement des données de santé, toute opération impliquant l'utilisation de données de santé. Toutefois, certaines opérations médicales requièrent impérativement le traitement de ces données, c'est pourquoi le règlement prévoit de nombreuses exceptions à cette interdiction¹⁶⁴³. Ainsi, l'obtention du consentement de la personne ou les exceptions prévues par le règlement, telles que la prévention de la santé publique, la préservation des intérêts vitaux de la personne concernée, l'appréciation médicale, la médecine du travail, le respect du pourcentage légal d'emploi de personnes handicapées, ainsi que la gestion des systèmes et services de santé ou de protection sociale.

Récemment, en France, la CNIL a constaté des manquements aux règles sur la protection des données, notamment en matière de données de santé¹⁶⁴⁴ qui sont particulièrement protégées et doivent faire l'objet d'une vigilance renforcée. L'autorité française a pointé du doigt les manquements des organismes procédant à des recherches médicales à leurs obligations de réaliser une analyse d'impact sur la protection des données et d'informer correctement les personnes. En effet, tous les projets de recherche dans le domaine de la santé, à l'exception des études dites internes, nécessitant un traitement de données de santé, doivent faire l'objet d'une formalité préalable auprès de la CNIL. Ces projets doivent conformes à une méthodologie de référence ou être autorisés par la CNIL. Ces méthodologies imposent de réaliser une analyse d'impact sur la protection des données avant de démarrer la recherche. Cette dernière doit notamment évaluer les risques sur les droits et les libertés des personnes.

¹⁶⁴¹ CNIL, « Qu'est-ce qu'une donnée de santé ? », 2018, en ligne à URL : <https://www.cnil.fr/fr/quest-ce-ce-qu'une-donnee-de-sante> consulté le 25 juillet 2023.

¹⁶⁴² RGPD, article 9.

¹⁶⁴³ CNIL, « Qu'est-ce qu'une donnée de santé ? », 2018, en ligne à URL : <https://www.cnil.fr/fr/quest-ce-ce-qu'une-donnee-de-sante> consulté le 25 juillet 2023.

¹⁶⁴⁴ CNIL, « Données de santé : la CNIL rappelle à deux organismes de recherche médicale leurs obligations légales », Données de santé, 21 mars 2023, en ligne à URL : <https://www.cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-deux-organismes-de-recherche-medicale-leurs-obligations-legales> consulté le 26 juillet 2023.

Sous-section 2 – L’utilisation des données personnelles contre la propagation de la pandémie comme une confirmation de l’extension du domaine des données personnelles des passagers aériens

L’impact de la crise sanitaire sur l’utilisation des données personnelles des passagers aériens appellent des considérations sanitaires, politiques, mais aussi économiques et juridiques non moins importante comme la protection du droit fondamental au respect de la vie privée et la protection des données personnelles. L’objet des dossiers passagers sera amené à évoluer au gré des crises que traverse le monde avec des objectifs qui dépassent le commerce et la sécurité et intègrent la santé et la lutte contre la fraude fiscale. On assiste alors à un retour de l’État comme acteur de premier plan dans la mise en œuvre de politiques relatives aux données personnelles des passagers aériens.

§ 1 – L’évolution de l’objet de l’utilisation des données personnelles des dossiers passagers vers le domaine de la santé

La pandémie a été déclarée par l'OMS en mars 2020. Une propagation rapide du virus SARS-CoV-2, responsable de la maladie du Covid-19, a provoqué des millions de cas de contaminations et de décès à travers le monde¹⁶⁴⁵. Face à cette situation de crise sanitaire, de nombreux États, y compris la France, ont dû prendre des mesures pour tenter de contenir la propagation du virus et protéger la santé publique de leurs citoyens. Le législateur français, en votant la loi du 5 août 2021¹⁶⁴⁶, a mis une place des mesures contraignantes qui ont fait débat dans l’opinion publique française, dont certaines ont été censurées par le juge constitutionnel¹⁶⁴⁷. Le Gouvernement français a pris différentes mesures¹⁶⁴⁸ tout au long de la pandémie, telles que des confinements, des couvre-feux, des restrictions de déplacement, des fermetures temporaires d'établissements publics et privés, ainsi que des campagnes de vaccination pour lutter contre le Covid-19.

¹⁶⁴⁵ D. ROUCAUTE, « Covid-19, maladies non transmissibles, pollution : l’OMS dresse son bilan de la santé mondiale », *Le Monde*, 19 mai 2023, en ligne à URL : https://www.lemonde.fr/planete/article/2023/05/19/covid-19-maladies-non-transmissibles-pollution-l-oms-dresse-son-bilan-de-la-sante-mondiale_6173967_3244.html consulté le 31 juillet 2023.

¹⁶⁴⁶ Loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire.

¹⁶⁴⁷ Vie publique, « Loi du 5 août 2021 relative à la gestion de la crise sanitaire », Panorama des lois, 6 août 2021, en ligne à URL : <https://www.vie-publique.fr/loi/280798-loi-5-aout-2021-vaccination-obligatoire-pass-sanitaire-crise-covid-19> consulté le 31 juillet 2023.

¹⁶⁴⁸ Un justificatif de statut vaccinal concernant la covid-19 et un certificat de rétablissement à la suite d'une contamination par la covid-19 ont été imposés par la loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire.

La loi du 5 août 2021¹⁶⁴⁹ est venue répondre à l'évolution de la situation sanitaire en France à cette époque. Elle avait pour objet de fournir un cadre législatif spécifique afin de permettre la mise en œuvre de mesures de gestion de crise plus ciblées, telles que l'extension du pass sanitaire et l'obligation vaccinale pour certaines professions. Par ailleurs, cette loi prolongea le régime de l'état d'urgence sanitaire qui avait été mis en place par la loi du 31 mai 2021¹⁶⁵⁰ jusqu'au 30 septembre 2021. Ce régime post-crise autorisait le Premier ministre à limiter les déplacements et l'utilisation des transports collectifs et à imposer des mesures barrières dans les commerces.

L'objectif était de renforcer les mesures de prévention, de lutte et de contrôle contre la propagation du virus tout en prenant en compte les enjeux de santé publique et de libertés individuelles. En effet, le contexte¹⁶⁵¹ de la loi était marqué par la nécessité de trouver un équilibre entre la protection de la santé publique et le respect des droits fondamentaux des citoyens français, tout en étant capable d'adapter les mesures au contexte constamment évolutif de la pandémie. L'opposition qui traverse les débats sur les dossiers passagers entre la protection des droits fondamentaux et la préservation de la sécurité publique, ou dit autrement entre la protection de la collectivité et la préservation des droits de l'individu, était de retour mais ce sont les considérations sanitaires qui ont alors pris le dessus sur les considérations purement sécuritaires.

L'arsenal législatif du 5 août 2021¹⁶⁵² a eu des incidences sur les déplacements internationaux des citoyens français et des voyageurs qui souhaitaient se rendre en France. Ces mesures spécifiques en matière de déplacements internationaux ont évolué avec le temps en fonction de la situation sanitaire, pour finalement être retirées¹⁶⁵³. Cette loi a eu des incidences sur les déplacements internationaux pour plusieurs raisons. D'abord, elle prolongea le pass sanitaire dans certains lieux en France. Ainsi, un voyageur se rendant France était concerné par l'utilisation du pass sanitaire dans certains établissements publics. D'autres pays étrangers pouvaient exiger un pass sanitaire ou un certificat de vaccination pour les voyageurs en

¹⁶⁴⁹ Loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire.

¹⁶⁵⁰ Loi n° 2021-689 du 31 mai 2021 relative à la gestion de la sortie de crise sanitaire.

¹⁶⁵¹ Le Monde, « Passe sanitaire : débats électriques à l'Assemblée nationale », *Le Monde avec AFP*, 22 juillet 2021, en ligne à URL : https://www.lemonde.fr/politique/article/2021/07/22/passe-sanitaire-les-deputes-prolongent-les-debats_6089126_823448.html consulté le 31 juillet 2023.

¹⁶⁵² Loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire, en ligne à URL : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043909676> consulté le 31 juillet 2023.

¹⁶⁵³ Vie publique, « Loi du 5 août 2021 relative à la gestion de la crise sanitaire », Panorama des lois, 6 août 2021, en ligne à URL : <https://www.vie-publique.fr/loi/280798-loi-5-aout-2021-vaccination-obligatoire-pass-sanitaire-crise-covid-19> consulté le 31 juillet 2023.

provenance de la France, comme les pays du Golfe¹⁶⁵⁴. Ainsi, les applications mobiles, requises par certains pays golfiotes pour permettre à un ressortissant étranger d'entrer sur leur territoire pendant la pandémie, ont été épinglées par la CNIL pour leur risque « d'espionnage »¹⁶⁵⁵.

La loi a également mis en place des restrictions de déplacements¹⁶⁵⁶, des interdictions de voyager dans certains pays ont été décidées et des quarantaines obligatoires à l'arrivée ont été imposées. D'autres mesures spécifiques ont permis aux autorités françaises de mettre en place des tests Covid-19 obligatoires dans les aéroports, avant le départ ou à l'arrivée, en fonction de la situation épidémique. La loi prévoyait également la vaccination obligatoire pour certaines professions en France. Le citoyen français ou le voyageur étranger exerçant l'une de ces professions pouvaient ainsi être concernés par des restrictions de ses déplacements internationaux s'il devait voyager alors que la vie durant le Covid-19 a été marqué par l'immobilisme pour reprendre les termes de différents spécialistes du secteur aériens¹⁶⁵⁷.

Cette activité législative¹⁶⁵⁸ marque en fait le retour de l'État dans la maîtrise de son territoire puisque la pandémie a eu pour conséquence que les frontières se sont renforcées dans un espace-temps au fur et à mesure que les gouvernements mettaient en place des politiques qui limitaient le mouvement des personnes. Les mesures prises par la plupart des États du monde ont démontré une volonté des gouvernements d'agir de manière autonome pour répondre à une urgence sanitaire en faisant appel à la capacité des autorités nationales à préserver la santé publique de leurs citoyens. Ce fait particulier nuance la thèse de Bertrand Badie¹⁶⁵⁹ sur la mondialisation qui engendre une crise de l'autorité traditionnelle de l'État-nation et de ses frontières puisque durant la pandémie, celles-ci sont redevenues pertinentes afin de permettre la maîtrise de la propagation du Covid-19. Conséquemment, les autorités étatiques ont davantage participé au traitement des données personnelles des passagers aériens en les

¹⁶⁵⁴ Gulf Times, « No Covid negative certificate needed for travellers from China », *Qatar*, 28 mars 2023, en ligne à URL : <https://www.gulf-times.com/article/658394/qatar/no-covid-negative-certificate-needed-for-travellers-from-china> consulté le 31 juillet 2023.

¹⁶⁵⁵ A. DEIANA, « Coupe du monde au Qatar : la Cnil conseille aux supporters français d'utiliser des téléphones vierges pour prévenir les risques d'espionnage », *France Info*, 15 novembre 2022, en ligne à URL : https://www.francetvinfo.fr/coupe-du-monde/coupe-du-monde-au-qatar-la-cnil-conseille-aux-supporters-francais-d-utiliser-des-telephones-vierges-pour-prevenir-les-risques-d-espionnage_5478510.html consulté le 31 juillet 2023.

¹⁶⁵⁶ Ministère de l'intérieur et des outre-mer, « Covid-19 : déplacements internationaux », 1^{er} août 2022, en ligne à URL : <https://www.interieur.gouv.fr/covid-19/deplacements-internationaux> consulté le 31 juillet 2023.

¹⁶⁵⁷ V. BONED, B. CRESPIEN, O. KERVILLA et autres, « La crise sanitaire : accélérateur de changement dans le tourisme », *Juris Tourisme*, Activités touristiques, Dalloz, n° 240, 2021, p. 39.

¹⁶⁵⁸ Loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire

¹⁶⁵⁹ B. BADIE, *La fin des territoires*, Fayard, 1995.

utilisant comme un moyen de maîtriser les flux des personnes entrant et sortant de leur territoire.

Cette reterritorialisation partielle est en fait un processus par lequel des flux auparavant mondialisés, opérant au-delà des frontières nationales, reviennent à des espaces spécifiques. Concrètement, l'État qui avait externalisé certaines de ses fonctions a décidé de les reprendre en charge au niveau national. On peut parler de reterritorialisation de la sécurité à travers l'utilisation des données à caractère personnel afin de tracer les individus qui entrent et ceux qui sortent du territoire dans un contexte de crise sanitaire mondiale. La notion de « reterritorialisation de la sécurité » est associée à la sociologue néerlandaise-américaine Saskia Sassen qui l'a développée en 2006 dans son ouvrage intitulé *Territoire, autorité, droits : de l'émiettement du pouvoir aux nouvelles échelles* (en anglais : *Territory, Authority, Rights: From Medieval to Global Assemblages*)¹⁶⁶⁰.

Dans cet essai, Saskia Sassen analyse les bouleversements qui se produisent dans les relations de pouvoir et les structures territoriales à l'ère de la mondialisation¹⁶⁶¹. La chercheuse soutient que malgré la montée de la mondialisation et la déterritorialisation apparente des processus économiques, politiques et sociaux, il existe également des phénomènes de reterritorialisation, y compris dans le domaine de la sécurité. Elle aborde notamment la manière dont certaines fonctions de sécurité, autrefois externalisées ou confiées à des acteurs internationaux, peuvent être reterritorisées au niveau national. Elle explique comment les États, en réponse à des menaces transnationales telles que le terrorisme ou la cybercriminalité¹⁶⁶², cherchent à reprendre le contrôle et à renforcer leurs capacités de sécurité à l'intérieur de leurs frontières.

La crise sanitaire est venue confirmer cette dynamique de reterritorialisation. En Grande-Bretagne¹⁶⁶³, alors que le Brexit était achevé, le gouvernement a exprimé son intention d'introduire un certificat de vaccination auquel il a dû renoncer. Toutefois, l'Écosse l'a introduit pour son territoire le 1^{er} octobre 2021. Dans l'espace britannique, les voyageurs

¹⁶⁶⁰ S. SASSEN, *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton, 2006.

¹⁶⁶¹ P. KANTOR, "Territory, Authority, Rights: From Medieval to Global Assemblages by Saskia Sassen", *Political Science Quarterly*, 2007, en ligne à URL : https://www.researchgate.net/publication/259814850_Territory_Authority_Rights_From_Medieval_to_Global_Assemblages_by_Saskia_Sassen consulté le 2 août 2023.

¹⁶⁶² I. BOUHADANA, W. GILLES, « Introduction – cyberspace, cybercriminalité & libertés », Irène Bouhadana, William Gilles (sous la direction de), *Cybercriminalité, cybermenaces & cyberfraudes*, Les éditions IMOD-V, Mars 2012, pp. 4-5. La diffusion généralisée du numérique dans les sociétés contemporaines, ainsi que la dématérialisation des documents courants, s'accompagnent de la propagation de la cybercriminalité avec de nouveaux types de menaces délictuelles.

¹⁶⁶³ Le Figaro, « Covid-19 : le gouvernement britannique renonce au passeport vaccinal », *Le Figaro avec AFP*, 12 septembre 2021, en ligne à URL : <https://www.lefigaro.fr/international/covid-19-le-gouvernement-britannique-renonce-au-passeport-vaccinal-20210912> consulté le 2 août 2023.

doublement vaccinés en provenance de certains pays devaient se soumettre à un test PCR de dépistage deux jours au plus tard après leur arrivée sur le territoire¹⁶⁶⁴.

En France, le pass vaccinal est entré en vigueur le 24 janvier 2022¹⁶⁶⁵ et a pris fin le 14 mars 2022. Il concernait les personnes âgées de 16 ans et plus et consistait en la présentation numérique ou papier d'une preuve de schéma vaccinal complet¹⁶⁶⁶. Un certificat de rétablissement valide ou un certificat de contre-indication à la vaccination permettaient aussi de valider le pass. Ce pass vaccinal était exigé pour les lieux recevant du public dont les transports aériens interrégionaux¹⁶⁶⁷.

Cette reterritorialisation a cependant été partielle, car l'Union européenne a également mis en œuvre des mesures pour contenir la propagation du virus en faisant en sorte que les États membres appliquent une politique qui dépasse le cadre national. L'Union européenne a établi le certificat Covid numérique afin de « faciliter la libre circulation en toute sécurité » pendant la crise sanitaire¹⁶⁶⁸. Ce système européen de certification numérique a été adopté le 1^{er} juillet 2023 par l'OMS afin de mettre en place un système mondial qui avait pour objectif de « protéger les citoyens du monde entier contre les menaces sanitaires actuelles et futures, y compris les pandémies »¹⁶⁶⁹.

Ce système relève d'un partenariat numérique entre l'Union européenne et l'OMS qui ont convenu de s'associer dans le domaine de la santé numérique afin de faciliter le développement et le fonctionnement du certificat numérique européen. Les deux organisations ont également signé un arrangement administratif¹⁶⁷⁰ non-contraignant en vue de collaborer à l'adoption du cadre du certificat numérique européen et de poursuivre le développement du réseau mondial de certification sanitaire numérique, qui est « un système volontaire qui peut

¹⁶⁶⁴ Ibidem

¹⁶⁶⁵ Loi n° 2022-46 du 22 janvier 2022 renforçant les outils de gestion de la crise sanitaire et modifiant le code de la santé publique.

¹⁶⁶⁶ Le ministère de l'Economie des finances et de la souveraineté industrielle et numérique, « Pass vaccinal : toutes les informations », 8 mars 2022, en ligne à URL : <https://www.economie.gouv.fr/pass-vaccinal-informations#> consulté le 2 août 2023.

¹⁶⁶⁷ Ibidem

¹⁶⁶⁸ Règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19. Voir en ce sens : Commission européenne, « Certificat COVID numérique de l'UE », Union européenne, *Communication*, 31 janvier 2022, en ligne à URL : https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_fr consulté le 2 août 2023.

¹⁶⁶⁹ Règlement, op. cit.

¹⁶⁷⁰ European Commission, « Administrative arrangement between the WHO and the European Commission on technical cooperation related to the global digital health certification network », 11 juillet 2023, en ligne à URL : https://commission.europa.eu/document/d1fb7b2e-0966-4496-a56a-5ab4a35ab15f_en consulté le 2 août 2023.

aider les citoyens européens à valider leurs documents de santé », et utiliser les données électroniques relatives à leur santé de manière sûre.

Ce pass sanitaire européen, adopté le 1^{er} juillet 2023¹⁶⁷¹, a été présenté comme le premier pas pour la mise en place d'un réseau mondial de certification sanitaire numérique de l'OMS qui aspire à mettre en place un système de vérification mondiale des documents sanitaires dans le but d'améliorer la santé des citoyens du monde entier¹⁶⁷². Ce processus qui se développe à l'échelle mondiale est un moyen pour l'OMS de faire converger les certificats numériques relatifs au Covid-19, d'adopter les normes européennes et de valider les signatures numériques dans l'objectif de prévenir la fraude. Toutefois, l'OMS n'a accès à aucune donnée à caractère personnel qui doivent rester du domaine exclusif des gouvernements nationaux.

Pour les autorités européennes, le certificat Covid numérique a été un pilier de la réponse de l'Union européenne à la pandémie. Plus de 2,3 milliards de certificats ont été délivrés¹⁶⁷³. Ce certificat couvrait les tests, la vaccination et les rétablissements dans le cadre de l'épidémie et a permis aux citoyens de voyager en toute sécurité. Il a également été présenté comme un moyen indispensable pour soutenir le secteur du tourisme européen qui a été durement touché par la crise épidémique.

Le document permettait aux citoyens de voyager en toute sécurité dans l'espace européen lorsque les États membres restreignaient les déplacements pour des raisons de santé publique. Cela a aidé également à coordonner la suppression des restrictions le plus rapidement possible¹⁶⁷⁴. De fait, depuis août 2022, il n'y a eu aucune restriction de mouvement au sein de l'Union européenne.

Le certificat numérique européen a également été un succès mondial selon les autorités européennes puisqu'il aurait établi une norme mondiale pour les voyages internationaux et il s'agit du seul système qui fonctionne à l'échelle internationale ; pas moins de 51 pays sur quatre continents ont bénéficié du système. Dans un rapport publié le 11 janvier 2023¹⁶⁷⁵, la Cour des comptes européenne estimait que le pass sanitaire de l'Union européenne avait rempli son rôle en facilitant les voyages pendant la pandémie du Covid-19. En effet, presque

¹⁶⁷¹ Règlement, op. cit.

¹⁶⁷² Commission européenne, « Certificat COVID numérique de l'UE », Union européenne, Communication, 31 janvier 2022, en ligne à URL : https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_fr consulté le 2 août 2023.

¹⁶⁷³ Ibidem

¹⁶⁷⁴ Ibid.

¹⁶⁷⁵ Cour des comptes, « Rapport public annuel 2023 », mars 2023. Voir en ce sens : Toute l'Europe, « Covid-19 : le pass sanitaire européen a été efficace, selon un nouveau rapport », *Comprendre l'Europe*, 11 janvier 2023, en ligne à URL : <https://www.toutteleurope.eu/societe/covid-19-le-pass-sanitaire-europeen-a-ete-efficace-selon-un-nouveau-rapport/> consulté le 2 août 2023.

tous les États membres avaient alors levé leurs restrictions pour les voyageurs titulaires de ce pass numérique.

L'utilisation des données personnelles des voyageurs, notamment des passagers aériens, pour faciliter les voyages pendant la pandémie du Covid-19 montre de quelle manière les données à caractère personnel peuvent constituer un élément essentiel à la fois d'une politique de sécurité et d'une politique de santé. En utilisant ces données pour l'entrée et la sortie du voyageur d'un territoire donné, l'État renforce sa capacité à maîtriser les flux de personnes afin de se protéger contre une pandémie, après avoir utilisé ces données personnelles pour se protéger contre les infractions terroristes et les crimes transnationaux. Les données personnelles sont un outil au service de l'État-nation, dans une phase de reterritorialisation, certes partielle, pour garder la mainmise sur un élément régalien : la maîtrise des frontières.

L'utilisation des données personnelles des passagers aériens, des données des dossiers passagers et des données sanitaires des voyageurs marque une étape importante dans les transformations contemporaines des relations complexes de pouvoir et de structures territoriales à l'ère de la mondialisation. La crise du Covid-19 n'a toutefois pas mis en cause la mondialisation comme phénomène puisque le taux d'ouverture mondial a résisté¹⁶⁷⁶.

Les dossiers passagers restent jusqu'à aujourd'hui un outil de lutte contre le terrorisme et le crime transnational. Toutefois, la crise sanitaire a montré que les États étaient prêts à réunir d'autres types de données, dont les données de santé, pour lutter contre la propagation d'une pandémie. Cet épisode montre que les données des voyageurs aériens peuvent être utilisées, d'une manière étendue, dépassant le concept des dossiers passagers, pour des objectifs de santé publique.

Comme pour les dossiers passagers, l'équilibre entre la sécurité collective et la liberté individuelle se pose dans le monde, plus précisément dans l'espace européen, car les citoyens de l'Union refusent de voir leurs droits fondamentaux, dont la protection des données à caractère personnel, être sacrifiés sous l'autel de la sécurité collective, même sanitaire¹⁶⁷⁷. En effet, en France par exemple, le pass sanitaire a été vivement et sévèrement critiqué en raison des atteintes aux libertés fondamentales, dont celle d'aller et venir¹⁶⁷⁸.

¹⁶⁷⁶ V. VICARD, « Vers la fin de la mondialisation », *ENS Lyon*, 3 janvier 2023, en ligne à URL : <https://ses.ens-lyon.fr/articles/vers-la-fin-de-la-mondialisation> consulté le 2 août 2023.

¹⁶⁷⁷ E. MAUPIN, « Les libertés individuelles à l'épreuve de la sortie de crise sanitaire », *Droit fondamental et liberté publique*, Administratif, Dalloz, 6 septembre 2021, en ligne à URL : <https://www.dalloz-actualite.fr/flash/libertes-individuelles-l-epreuve-de-sortie-de-crise-sanitaire> consulté le 2 août 2023.

¹⁶⁷⁸ Ibidem

§ 2 – La probable utilisation contestée des dossiers passagers en tant qu’outil de lutte contre la fraude fiscale

La fraude fiscale est définie comme « l'opération consistant à se soustraire ou tenter de se soustraire frauduleusement à l'établissement ou au paiement total ou partiel de l'impôt, selon différentes modalités. Des éléments constitutifs permettent de caractériser le délit et de le poursuivre »¹⁶⁷⁹. Elle est accomplie lorsque deux éléments constitutifs sont réalisés, un élément matériel et un élément intentionnel selon le Code général des impôts (ci-après CGI). L'élément matériel requiert qu'il existe une « soustraction ou tentative de soustraction à l'établissement ou au paiement total ou partiel des impôts figurant dans le code général des impôts », précisément à l'article 1741¹⁶⁸⁰. Le législateur réprime tant la fraude fiscale que la tentative de la réaliser, tant en matière d'assiette que de recouvrement de l'impôt. Cette répression couvre aussi bien « les impôts directs, indirects, droits d'enregistrement et taxes assimilées que les taxes sur les chiffres d'affaires ou encore l'impôt sur la fortune immobilière »¹⁶⁸¹. L'élément intentionnel¹⁶⁸² quant à lui signifie que « l'auteur de l'infraction doit avoir eu l'intention délibérée de frauder ou de tenter de frauder ». La preuve du caractère intentionnel de l'infraction relève de la responsabilité du ministère public et de l'administration fiscale¹⁶⁸³⁻¹⁶⁸⁴. La fraude fiscale se décline en de multiples concepts avec des logiques différentes. André Barilari estime que les pertes fiscales en France s'évaluent entre 80 et 100 milliards d'euros¹⁶⁸⁵.

En 2023, le Gouvernement français a affiché sa volonté de lutter contre la fraude fiscale en utilisant les dossiers passagers. Pour le ministre délégué chargé des Comptes publics, l'exploitation de ces fichiers doit permettre de vérifier le temps passé sur le territoire de personnes indiquant qu'elles ne sont pas résidentes en France et de vérifier ainsi si les personnes notifiant aux services fiscaux qu'elles ne sont pas résidentes en France, et ne payant pas d'impôts, disent vrai¹⁶⁸⁶. Cette proposition s'inscrit dans le cadre de la présentation d'un

¹⁶⁷⁹ Dalloz, « Fraude fiscale », Fiche d'orientation, Dalloz, août 2022

¹⁶⁸⁰ Article L. 1741, CGI.

¹⁶⁸¹ Dalloz, « Fraude fiscale », Fiche d'orientation, Dalloz, août 2022.

¹⁶⁸² Ibidem

¹⁶⁸³ Article L. 227, Livre des procédures fiscales.

¹⁶⁸⁴ Crim. 25 mai 1987, n° 85-95.191.

¹⁶⁸⁵ A. BARILARI, « La fraude fiscale : les mots et les chiffres », *Gestion et finances publiques*, 2018/3 (n° 3), pp. 50-57, 2018, en ligne à URL : <https://www.cairn.info/revue-gestion-et-finances-publiques-2018-3-page-50.htm> consulté le 3 août 2023.

¹⁶⁸⁶ M. FODÉRE, « Le gouvernement veut interroger les compagnies aériennes pour traquer les fraudeurs fiscaux », *Europe 1*, 10 mai 2023, en ligne à URL : <https://www.europe1.fr/economie/le-gouvernement-veut-interroger-les-compagnies-aeriennes-pour-traquer-les-fraudeurs-fiscaux-4182388> consulté le 4 août 2023.

plan gouvernemental de lutte contre la fraude fiscale, notamment la fraude internationale¹⁶⁸⁷. Le Gouvernement souhaite ainsi, au moyen de l'utilisation des données des dossiers passagers, savoir à quel moment une personne a pris l'avion et à quel moment elle est revenue en France. Cette annonce a ramené ces données au centre de l'attention de l'opinion publique, permettant ainsi de les exploiter sous un angle nouveau.

Pour l'administration fiscale, l'accès aux données PNR présente un intérêt majeur ; celui d'assurer que le bénéficiaire d'une prestation sociale réside bien sur le sol français. En droit français, il convient de justifier d'une résidence d'au moins six mois en France pour toucher le minimum vieillesse et les allocations familiales, huit mois pour bénéficier de l'aide personnalisée au logement (ci-après APL) et neuf mois pour être éligible au revenu de solidarité active (ci-après RSA). Auparavant, ces opérations étaient réalisées manuellement, rendant lourde toute exploitation de données.

Ces données des dossiers passagers donneraient à l'administration fiscale la capacité de vérifier qu'un bénéficiaire d'une prestation sociale conditionnée à sa résidence en France ne se trouve pas en réalité hors du territoire français, ou encore de vérifier la durée effectivement passée sur le territoire hexagonal d'une personne ayant déclaré ne pas avoir résidence sur le sol français pour bénéficier d'une législation fiscale plus généreuse. L'objectif est de permettre l'accès aux informations liées à la réservation du billet d'avion. Ces données sont détenues par la compagnie aérienne. Elles incluent l'itinéraire du voyage et les vols concernés. Elles couvrent aussi les coordonnées du passager au sol comme les numéros de téléphone personnel et professionnel. Les informations sur les tarifs appliqués et l'état du paiement en font également partie. Le numéro de carte bancaire du passager est aussi concerné. Enfin, elles incluent les services demandés à bord, comme les préférences alimentaires ou les services liés à la santé du passager¹⁶⁸⁸.

Pour l'administration, l'intérêt porté aux données PNR semble résider dans le fait que ces dernières sont disponibles avant les données API, offrant ainsi aux autorités répressives de chaque État une facilité pour les traiter, les analyser et ainsi prendre toute mesure jugée nécessaire comme l'interpellation d'une personne recherchée¹⁶⁸⁹. Ces données se

¹⁶⁸⁷ AFP, « Fraude fiscale : le gouvernement cible les 'ultra-riches' et les multinationales », *Europe 1*, 10 mai 2023, en ligne à URL : <https://www.europe1.fr/economie/le-gouvernement-souhaite-augmenter-de-25-les-controles-fiscaux-des-plus-gros-patrimoines-4182063> consulté le 4 août 2023.

¹⁶⁸⁸ CNIL, « Passenger Name Record », Définition, en ligne à URL : <https://www.cnil.fr/fr/definition/pnr-passenger-name-record> consulté le 4 août 2023.

¹⁶⁸⁹ S. OMARJEE, J. BELOT, « L'accès au PNR pour lutter contre la fraude fiscale : une nouvelle menace pour la vie privée ? », *Village de la justice*, en ligne à URL : <https://www.village-justice.com/articles/acces-pnr-pour-lutter-contre-fraude-fiscale-une-nouvelle-menace-pour-vie->

Toutes les informations nécessaires au voyage sont conservées dans le système de réservation et de contrôle des départs, puis sont échangées auprès de tous les acteurs du secteur aérien. Ainsi, les autorités sécuritaires ont la possibilité de reconstituer tous les déplacements aériens du passager et même réaliser un profilage précis de ce dernier. Les progrès technologiques permettent désormais de traiter ces données électroniquement presque instantanément et de les utiliser comme outil de renseignement pour une activité criminelle potentielle¹⁶⁹⁰.

L'association de la fraude fiscale à une forme grave de criminalité pourrait se heurter à différents textes juridiques dont le premier est le RGPD. En effet, comme tout fichier regroupant des données personnelles permettant d'identifier directement ou indirectement une

¹⁶⁹² 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.

personne physique, le dossier passager doit respecter la législation européenne sur les données à caractère personnel.

Pour Sulliman Omarjee, l'utilisation des données PNR dans la lutte contre la fraude fiscale pourrait fort bien se heurter aux principes de finalité et de légalité de la collecte qui innervent le RGPD¹⁶⁹³.

L'article 5 du règlement impose que les données à caractère personnel soient traitées de manière licite, loyale et transparente vis-à-vis de la personne concernée. Elles doivent également être collectées pour des finalités déterminées, explicites et légitimes, sans traitement ultérieur incompatible avec ces finalités. Par ailleurs, l'article L. 232-7 du Code de la sécurité intérieure, qui transpose la directive PNR, établit un traitement des données ayant pour finalité la prévention et la constatation de certaines infractions, notamment les actes de terrorisme, les atteintes aux intérêts fondamentaux de la nation ainsi que les infractions listées à l'annexe II de la directive (UE) 2016/681.

Bien que l'annexe II de la directive contienne un point 7 qui prévoit « la fraude portant atteinte aux intérêts financiers de l'Union », il est peu probable pour Sulliman Omarjee que le séjour hors de France d'un individu qui continue de percevoir ses allocations remplit la condition de gravité permettant que sa situation se rattache à cette disposition. Les transporteurs aériens doivent communiquer les données des passagers enregistrées dans leurs systèmes de réservation uniquement si cette condition est remplie¹⁶⁹⁴.

En l'état actuel du droit, l'objet du PNR n'est pas de lutter contre la fraude fiscale. Par conséquent, le recoupement de tout fichier entre l'autorité en charge du PNR et l'administration fiscale recevant le PNR est illégal. Si les autorités fiscales pouvaient accéder aux données PNR dans le but de traquer les fraudeurs, un tel accès constituerait un détournement des finalités au sens du RGPD. Les autorités fiscales ne sont pas non plus indiquées comme destinataires des données, cette transmission pourrait donc constituer une faille de sécurité. Si elle est justifiée, la création d'un fichier fourni par les données PNR constituerait une collecte illicite déloyale. L'accès au PNR est donc strictement réglementé et les compagnies aériennes ne sont tenues de fournir ces données que dans les cas prévus expressément par la loi. En d'autres termes, du point de vue du droit européen, comme du

¹⁶⁹³ S. OMARJEE, J. BELOT, « L'accès au PNR pour lutter contre la fraude fiscale : une nouvelle menace pour la vie privée ? », *Village de la justice*, en ligne à URL : [https://www.village-justice.com/articles/acces-pnr-pour-lutter-contre-fraude-fiscale-une-nouvelle-menace-pour-vie-privee,46364.html#:~:text=L'annonce%20du%20ministre%20des,PNR%20\(Passengers%20Names%20Record\)](https://www.village-justice.com/articles/acces-pnr-pour-lutter-contre-fraude-fiscale-une-nouvelle-menace-pour-vie-privee,46364.html#:~:text=L'annonce%20du%20ministre%20des,PNR%20(Passengers%20Names%20Record)) consulté le 4 août 2023.

¹⁶⁹⁴ Ibidem

droit français, les compagnies aériennes doivent refuser toute transmission des données des dossiers passagers à l'administration fiscale au risque d'enfreindre ces droits.

Le projet d'élargissement de l'accès aux PNR précédemment mentionné est inquiétant puisqu'il ressemblera à une surveillance généralisée des citoyens français, dépassant le suivi des passagers, dont les données seraient croisées avec des données détenues par le fisc ou les caisses de sécurité sociale. Toute personne interrogée devrait alors justifier sa situation, ce qui peut engendrer des atteintes illégitimes aux droits fondamentaux des personnes¹⁶⁹⁵. Il n'est pas certain que de telles infractions soient proportionnées à ce qui est poursuivi. S'il est concevable que la lutte contre le terrorisme et les formes graves de criminalité puisse justifier que les autorités judiciaires obtiennent ces données des passagers aériens pour assurer la sécurité des personnes, la lutte contre l'évasion fiscale est loin de constituer une finalité aussi sérieuse et la conciliation entre lutte contre la fraude fiscale et le respect des droits fondamentaux, dont la protection des données personnelles, est loin d'être acquise. C'est ce que la CNIL a rappelé en considérant que le système PNR « pouvait porter une atteinte grave au respect de la vie privée, en raison du grand nombre de personnes concernées et de la quantité d'informations enregistrées »¹⁶⁹⁶.

La CJUE a aussi eu l'occasion de se prononcer sur cette question dans un arrêt du 21 juin 2022¹⁶⁹⁷ portant sur la directive PNR de 2016, en réaffirmant les contours précis et limités de tout transfert de données des passagers. Selon le droit de l'Union européenne, en particulier l'article 2 de la directive PNR¹⁶⁹⁸, une législation nationale ne peut prévoir un système de transfert et de traitement des données PNR pour tous les vols intra-UE et autres moyens de transport au sein de l'Union en l'absence d'une menace terroriste réelle, actuelle ou prévisible. Ces transfert et traitement par les autorités compétentes ne sont autorisés que dans le cadre de la lutte contre les infractions terroristes et les formes graves de criminalité¹⁶⁹⁹.

La Cour a précisé que lorsqu'une menace apparaît, l'application du système prévu par la directive PNR doit se limiter au transfert et au traitement des données PNR des vols et transports spécifiques. Cela concerne notamment certaines liaisons, schémas de voyage ainsi

¹⁶⁹⁵ P. AIGRAIN, « Porte ouverte à la surveillance et à la suspicion généralisées », *Dalloz*, Pénal, 24 mars 2015, en ligne à URL : <https://www.dalloz-actualite.fr/chronique/porte-ouverte-surveillance-et-suspicion-generalisees> consulté le 5 août 2023.

¹⁶⁹⁶ CNIL, délibération 2014-308 du 17 juillet 2014 portant avis sur un projet de décret relatif à la création d'un traitement de données à caractère personnel dénommé « système API-PNR France » pris pour l'application de l'article L. 232-7 du code de la sécurité intérieure et fixant les modalités de transmission au service à compétence nationale « Unité Information Passagers » des données relatives aux passagers par les transporteurs aériens.

¹⁶⁹⁷ CJUE, 21 juin 2022, affaire C-817/19.

¹⁶⁹⁸ Directive PNR, article 2.

¹⁶⁹⁹ CJUE, 21 juin 2022, affaire C-817/19.

que certains aéroports, gares, ou ports maritimes pour lesquels des indications justifient cette application¹⁷⁰⁰. Le juge européen a donc été on ne peut plus clair sur le fait que la transmission des fichiers PNR ne peut être justifiée qu'en raison de l'existence d'une menace qui soit réelle et non hypothétique¹⁷⁰¹ tout en précisant clairement que « le droit de l'Union s'oppose à une législation nationale prévoyant un tel système de transfert et de traitement desdites données aux fins de l'amélioration des contrôles aux frontières et de la lutte contre l'immigration clandestine »¹⁷⁰².

Pour Me Omarjee, la lutte contre la fraude fiscale ne peut justifier encore plus de restrictions vis-à-vis des droits fondamentaux des citoyens, notamment ceux de la protection de la vie privée et de la liberté de circulation. Ce dernier craint « un étau qui se resserre progressivement autour du citoyen à qui l'on intime de se justifier, au risque de piétiner davantage sa vie privée en contrôlant ses déplacements »¹⁷⁰³. Il a également tenu à souligner la contradiction entre la volonté affichée de protéger les données personnelles des citoyens et le fait de dénier leurs droits pour des raisons de sécurité. Selon lui, étendre l'accès aux données PNR aux autorités fiscales signifierait réduire davantage la vie privée de chacun lors de ses déplacements. En effet, la protection du droit de chacun au respect de sa vie privée et à sa liberté de circulation est essentielle dans une société démocratique où la technologie peut permettre aux pouvoirs publics d'employer de nouveaux moyens de surveillance contre chacun, suscitant la crainte d'une surveillance de masse.

L'utilisation des données PNR dans le cadre de la lutte contre le terrorisme et la criminalité grave avait été rendue possible, parce que le contexte des attentats de New York du 11 septembre 2001 et de Paris du 13 novembre 2015 avait encouragé les États membres de l'Union, dont la France, à adopté une nouvelle législation réglementant cette transmission vers le sol américain selon un cadre strict afin de préserver les droits des citoyens européens. Les institutions européennes et la CJUE avaient ensuite encadré davantage cette transmission afin de ne pas sacrifier les droits fondamentaux des citoyens européens sous l'autel de la

¹⁷⁰⁰ Ibidem

¹⁷⁰¹ S. OMARJEE, J. BELOT, « L'accès au PNR pour lutter contre la fraude fiscale : une nouvelle menace pour la vie privée ? », *Village de la justice*, en ligne à URL : [https://www.village-justice.com/articles/acces-pnr-pour-lutter-contre-fraude-fiscale-une-nouvelle-menace-pour-vie-privee,46364.html#:~:text=L'annonce%20du%20ministre%20des,PNR%20\(Passengers%20Names%20Record\)](https://www.village-justice.com/articles/acces-pnr-pour-lutter-contre-fraude-fiscale-une-nouvelle-menace-pour-vie-privee,46364.html#:~:text=L'annonce%20du%20ministre%20des,PNR%20(Passengers%20Names%20Record)) consulté le 4 août 2023.

¹⁷⁰² CJUE, 21 juin 2022, aff. C-817/19.

¹⁷⁰³ S. OMARJEE, J. BELOT, « L'accès au PNR pour lutter contre la fraude fiscale : une nouvelle menace pour la vie privée ? », *Village de la justice*, en ligne à URL : [https://www.village-justice.com/articles/acces-pnr-pour-lutter-contre-fraude-fiscale-une-nouvelle-menace-pour-vie-privee,46364.html#:~:text=L'annonce%20du%20ministre%20des,PNR%20\(Passengers%20Names%20Record\)](https://www.village-justice.com/articles/acces-pnr-pour-lutter-contre-fraude-fiscale-une-nouvelle-menace-pour-vie-privee,46364.html#:~:text=L'annonce%20du%20ministre%20des,PNR%20(Passengers%20Names%20Record)) consulté le 4 août 2023.

sécurité collective en considérant que le transfert de ces données ne pouvait se faire qu'en présence d'une « menace terroriste réelle et actuelle ou prévisible » à laquelle ferait face un État membre. Elles ont également alerté sur les craintes d'un régime de surveillance « continu, non ciblé et systématique », incluant l'évaluation automatisée de données à caractère personnel de l'ensemble des personnes faisant usage du transport aérien, et affirmé que le traitement des données personnelles des passagers aériens devra toujours faire l'objet d'une limitation à ce qui est « strictement nécessaire » au regard des objectifs visés de lutte contre le terrorisme et des formes graves de criminalité¹⁷⁰⁴.

Aujourd'hui, les risques d'atteintes aux intérêts fondamentaux de la nation n'englobent pas encore la fraude fiscale. Ces intérêts fondamentaux sont, selon le Code pénal français à l'article 410-1, comme « son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel »¹⁷⁰⁵.

Dans ses observations sur la loi relative au renseignement, le Gouvernement avait limité les « menaces immédiates » à l'indépendance nationale, l'intégrité du territoire et la défense nationale, la prévention des actes de terrorisme et la prévention des atteintes à la forme républicaine des institutions¹⁷⁰⁶. Bien qu'elle soit un enjeu important pour les gouvernements afin de garantir l'intégrité du système fiscal et le maintien de l'équité entre les contribuables, la lutte contre la fraude fiscale n'est pas considérée par le droit français comme une atteinte aux intérêts fondamentaux de la nation justifiant une utilisation extensive des données des dossiers passagers dans la lutte contre les objectifs que les droits européen et français ont prévu.

¹⁷⁰⁴ G. HAAS, A-C. ANDRIEUX, S. BAKLI, « Directive PNR : la CJUE recadre le traitement des données de passagers aériens », *HAAS avocats*, 16 août 2022, en ligne à URL : <https://info.haas-avocats.com/droit-digital/directive-pnr-la-cjue-recadre-le-traitement-des-donnees-de-passagers-aeriens> consulté le 5 août 2023.

¹⁷⁰⁵ Code pénal, article 410-1.

¹⁷⁰⁶ Légifrance, « Observations du Gouvernement sur la loi relative au renseignement », *Journal officiel électronique authentifié*, 26 juillet 2015, en ligne à URL : <https://www.legifrance.gouv.fr/jorf/id/JORFARTI000030932377#JORFARTI000030932377> consulté le 5 août 2023.

Section 2 – Vers une harmonisation difficile du régime national des dossiers passagers : une conséquence de la crise du multilatéralisme

Le concept de multilatéralisme est, en général, associé à la concertation pacifique entre au moins trois États dans un cadre dont les contours sont tracés en commun¹⁷⁰⁷. L'Organisation des Nations Unies en est l'exemple le plus connu mais il n'est pas le seul. L'effort multilatéral qui en découle peut concerner divers domaines dont la sécurité, le commerce, la justice pénale, les droits de l'Homme, l'environnement, le numérique, ou bien la santé. Pourtant, les différents cadres et institutions créés, depuis le début du XX^e siècle, se portent mal. Le multilatéralisme connaît depuis quelques années une crise multifactorielle et multidimensionnelle (sous-section 1) qui est le reflet d'un monde en fragmentation au carrefour de différentes transformations.

L'harmonisation des législations apparaît nécessaire au développement de la protection des données à caractère personnel des passagers aériens (sous-section 2). Elle se situe entre l'unification des règles de droit et une simple compatibilité des systèmes juridiques. L'action d'harmonisation requiert de dégager des directions et des orientations communes ainsi que d'établir des principes et des règles sur la base d'une compréhension commune des enjeux de protection des données personnelles¹⁷⁰⁸. Si l'harmonisation est effectivement indissociable de la codification et de la modernisation du droit, alors il ne faut pas chercher à tout harmoniser ni à harmoniser par tous les moyens selon le Professeur François Collard Dutilleul¹⁷⁰⁹. Ainsi, les règles d'inspiration culturelle, comme le droit des personnes, qui émergent de l'histoire d'un pays ou d'une région doivent conserver leur spécificité¹⁷¹⁰. En effet, l'uniformisation des différentes cultures, l'évolution des mœurs, l'affaiblissement de l'influence des traditions peuvent concourir à plus d'harmonisation dans le droit. Au contraire, les lois relatives au règlement des différends exigent une coordination volontaire et spécifique. Il semble en aller de même pour le droit à la protection des données à caractère personnel.

¹⁷⁰⁷ J. FERNANDEZ, J.-V. HOLEINDRE, *Nations désunies ? La crise du multilatéralisme dans les relations internationales*, CNRS, Biblis Inédit, 7 avril 2022.

¹⁷⁰⁸ F. COLLARD DUTILLEUL, « L'harmonisation internationale du droit privé », *Revue générale de droit, Droit comparé*, Volume 24, Numéro 2, 2 juin 1993, en ligne à URL : <https://id.erudit.org/iderudit/1056952ar> consulté le 7 août 2023.

¹⁷⁰⁹ Ibidem

¹⁷¹⁰ J.-M. DEFAYS, « Harmoniser les cultures, orchestrer la communication dans la classe et en dehors », *Mardaga*, PSY-Théories, débats, synthèses, in *Enseigner le français – Langue étrangère et seconde, approche humaniste de la didactique des langues et des cultures*, 2018.

À cet égard, les organisations internationales ou les entités *sui generis* comme l'Union européenne¹⁷¹¹ jouent un rôle important pour parvenir à la coordination entre les États membres¹⁷¹². La directive de l'Union européenne relative aux données des dossiers passagers, adoptée par le Conseil le 21 avril 2016, apparaît comme l'incarnation d'une volonté commune des États membres de réglementer le transfert des données des dossiers passagers, par les compagnies aériennes aux autorités nationales, ainsi que le traitement desdites données. Cette législation européenne encadre le transfert de ces données aux autorités répressives des États membres et leur traitement « aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité ainsi que des enquêtes et des poursuites en la matière »¹⁷¹³.

Bien que la plupart des États membres utilisaient déjà ces données transmises à la police ou à d'autres autorités en vertu du droit national, le système PNR européen a harmonisé les lois nationales des États membres dans le but d'éviter une insécurité juridique et des failles en matière de sécurité, tout en aspirant à garantir la protection des données à caractère personnel¹⁷¹⁴. En effet, les autorités européennes ont souhaité contrer la menace que représentent le terrorisme et la grande criminalité ainsi que les risques liés à la suppression des contrôles aux frontières intérieures en application de la Convention de Schengen, en adoptant des mesures organisant la collecte des données personnelles et l'échange de celles-ci entre autorités répressives et d'autres services. La mise en place du PNR européen souligne la volonté d'accroître la coopération entre les services répressifs à l'égard des passagers de vols internationaux en utilisant systématiquement les données des dossiers passagers dans un contexte international¹⁷¹⁵ encore marqué par les attentats du 11 septembre 2001, le projet d'attentat aérien déjoué d'août 2006 entre le Royaume-Uni et les États-Unis et la tentative d'attentat à bord de vol Amsterdam-Detroit en décembre 2009.

¹⁷¹¹ S. HENRY, « L'Union européenne, une construction *sui generis* », Ellipses, Droit de l'Union européenne, Tout-en-un droit, 2020, p. 28 à 42, en ligne à URL : <https://www.cairn.info/droit-de-l-union-europeenne--9782340036079.htm> consulté le 7 août 2023.

¹⁷¹² T. RAMBAUD, « Le rapprochement des grandes traditions juridiques dans le monde », Presses Universitaires de France, Quadriga, Introduction au droit comparé, p. 237 à 291, 2014, en ligne à URL : <https://www.cairn.info/introduction-au-droit-compare--9782130624554.htm> consulté le 7 août 2023.

¹⁷¹³ 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.

¹⁷¹⁴ Commission européenne, « Proposition de Directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers 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 », Union européenne, Dossier interinstitutionnel : 2011/0023, Bruxelles, 4 février 2011.

¹⁷¹⁵ Ibidem

Sous-section 1 – La protection juridique des dossiers passagers face une myriade d’accords caractérisés par un déficit d’harmonisation

§ 1 – L’absence d’un droit aérien international contraignant vis-à-vis des données des dossiers passagers.

Au regard du droit aérien international, les données PNR sont régies par l'Annexe 9 à la Convention de Chicago¹⁷¹⁶ qui a trait à la « facilitation »¹⁷¹⁷. Ce concept de « facilitation » découle de l'article 22 de la Convention de Chicago qui prévoit, sous le titre « simplification des formalités » que « chaque État contractant convient d'adopter, par la promulgation de règlements spéciale ou de toute autre manière, toutes mesures en son pouvoir pour faciliter et accélérer la navigation par aéronef entre les territoires des États contractants et éviter de retarder sans nécessité les aéronefs, équipages, passagers et cargaisons, particulièrement dans l'application des lois relatives à l'immigration, à la santé, à la douane et au congé »¹⁷¹⁸.

De même, l'article 23 précise que « Chaque État contractant s'engage, dans la mesure où il le juge réalisable, à établir des règlements de douane et d'immigration intéressantes la navigation aérienne internationale, conformément aux pratiques qui pourraient être établies ou recommandées en vertu de la présente Convention ». Ainsi, les normes et pratiques recommandées adoptées par l'OACI à l'Annexe 9 ne se prononcent pas sur la pertinence de la collecte et du traitement des données à caractère personnel des passagers aériens mais soulignent la volonté des États désireux d'utiliser ces données, en cherchant à encadrer, simplifier et faciliter leur échange. Cela explique pourquoi le Chapitre 9 qui les encadre est subrepticement intitulé « Systèmes d'échange de données sur les passagers ».

C'est, aussi pour cette raison qu'on ne trouve aucune mention explicite desdites données à l'Annexe 17, pourtant consacrée à la sûreté aérienne¹⁷¹⁹. Cette dernière porte principalement sur les inspections, inspections/filtrages et autres contrôles de sûreté, au sol comme à bord des aéronefs. Elle vise ainsi tant les « mesures pour empêcher que des armes, explosifs ou tout autres engins, articles ou substances dangereuses pouvant être employés pour commettre un acte d'intervention illicite, et dont le port ou le transport n'est pas autorisé, ne soient introduits, par quelque moyen que ce soit, à bord d'un aéronef effectuant un vol d'aviation civile »¹⁷²⁰

¹⁷¹⁶ Convention relative à l'aviation civile internationale, Chicago, 7 décembre 1944.

¹⁷¹⁷ V. CORREIA, « Données des passagers aériens », *Jurisclasseur Communication*, LexisNexis, 15 novembre 2019.

¹⁷¹⁸ Ibidem

¹⁷¹⁹ Annexe 17, Convention de Chicago, 10^e édition, 2017.

¹⁷²⁰ Ibidem, norme 4.1.1.

que le contrôle de l'accès aux pistes et zones réglementées, ou l'inspection des passagers, marchandises et bagages.

Mis à part quelques recommandations et standards, il n'y a pas eu de traité international encadrant et réglementant le transfert et le traitement des données des dossiers passagers (PNR).

1. L'Organisation de l'aviation civile internationale, une organisation édictant des recommandations sur les dossiers passagers aériens

Le 7 décembre 1944, une cinquantaine d'États ont adopté la Convention relative à l'aviation civile internationale, appelée également Convention de Chicago¹⁷²¹. Ce traité international a établi les bases du cadre réglementaire international pour l'aviation civile et créé l'Organisation de l'aviation civile internationale (OACI), devenue une agence spécialisée des Nations Unies chargée de promouvoir le développement de l'aviation civile internationale et sa sécurité.

La Convention de Chicago a établi des principes et des normes fondamentaux pour la sécurité aérienne, la navigation, la sûreté, la facilitation des déplacements aériens et la protection de l'environnement. Aussi, l'organisation a joué un rôle crucial dans la coordination entre les États signataires pour élaborer des normes et des recommandations uniformes dans le domaine de la réglementation de l'aviation civile dans le but de garantir des opérations efficaces et sûres à l'échelle mondiale. L'OACI a élaboré des codes de conduite pour la sécurité aérienne, des procédures de contrôle de la circulation aérienne, des règles relatives aux aéroports et aux installations aéronautiques tout en promouvant la coopération entre États afin de résoudre les enjeux liés à l'aviation civile internationale¹⁷²².

Discutées à l'occasion de la 12^e session de facilitation de l'OACI qui s'est tenue du 22 mars au 1^{er} avril 2004, les données des dossiers passagers (PNR) ont été intégrées pour la première fois à l'Annexe 9 de la Convention de Chicago en mars 2005. L'OACI collabore également avec l'Association internationale du transport aérien et l'Organisation mondiale des douanes dans ce domaine. Cela a notamment donné lieu à la publication conjointe de documents, sous

¹⁷²¹ B. MERCADAL, « Aviation », *Répertoire de droit commercial*, Dalloz, novembre 2017.

¹⁷²² On peut citer : OACI, Annexe 17 à la Convention relative à l'aviation civile internationale – Sécurité : protection de l'aviation civile internationale contre les actes d'intervention illicite, 2017, OACI, Manuel de gestion de la sécurité (Safety Management Manual – SMM), 2018.

la forme de lignes directrices ou autres instruments de *soft law* dont des lignes directrices en 2014 (Guidelines on Advance Passenger Information, 2014)¹⁷²³.

2. *L'Association du transport aérien international, une organisation édictant des standards sur les dossiers passagers aériens*

L'International Air Transport Association ou Association du transport aérien international (ci-après IATA) a été instituée par les membres de l'OACI. Cette association privée, en accord avec le statut coopératif canadien, siège à Montréal¹⁷²⁴. Elle a pour mission, d'une part, l'harmonisation des conditions et des activités de transport, notamment la standardisation des techniques et, d'autre part, la coordination tarifaire. Pour Denis Broussolle, cette seconde mission a été battue en brèche par le développement du droit de l'Union européenne¹⁷²⁵ et la libéralisation du secteur du transporteur aérien, avec notamment la loi américaine Airline Deregulation Act (ADA), adoptée le 24 octobre 1979, qui a eu pour objectif de déréglementer l'industrie du transport aérien aux États-Unis. Avant l'adoption de cette dernière, l'industrie aérienne américaine était étroitement encadrée par le Gouvernement fédéral, notamment en ce qui concerne les routes, les tarifs, les horaires et d'autres aspects opérationnels. Certains critiques et experts estiment que cette libéralisation a entraîné des effets négatifs dont la réduction des coûts opérationnels, une source d'inquiétude pour les experts au regard de la sécurité des vols en raison de la pression constante pour réduire encore plus ces coûts¹⁷²⁶.

L'IATA, en tant qu'association des compagnies aériennes mondiales, a été activement impliquée dans les discussions et les initiatives liées au PNR. En effet, cette association a élaboré un format de message standardisé pour faciliter la transmission des données des passagers aux autorités gouvernementales. Le PNRGOV¹⁷²⁷ est ainsi utilisé pour permettre aux compagnies aériennes de transmettre des informations de voyage et de sécurité relatives aux passagers aux autorités compétentes, telles que les agences de sécurité et les services d'immigration, conformément aux lois en matière d'aviation.

En utilisant ce format, les compagnies aériennes peuvent ainsi répondre aux exigences de collecte et de transmission de données aux autorités gouvernementales, tout en garantissant la

¹⁷²³ OACI, Lignes directrices sur les données des dossiers passagers (PNR), 2014. Voir : V. CORREIA, « Données des passagers aériens », *Jurisque Communication*, LexisNexis, 15 novembre 2019.

¹⁷²⁴ D. BROUSSOLLE, « Société de transports », *Répertoire des sociétés*, Dalloz, décembre 2010.

¹⁷²⁵ Ibidem

¹⁷²⁶ R.B. EDELMAN, B. RICHARD, H. KENT BAKER, "The impact of implementing the airline deregulation act on stock returns", *Journal of Economics and Finance*, 1996, pp. 79-99.

¹⁷²⁷ IATA, *Passenger and airport data interchange standards*, PADIS XML Implementation Guide, PNRGOV Message, 2016, en ligne à URL : https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/pnrgov20xml20implementation20guide2016_1.pdf consulté le 9 août 2023.

protection de données des passagers aériens. Cela permet également aux autorités de disposer des informations nécessaires pour mener des vérifications de sécurité et de sûreté. Cependant, les détails spécifiques du format PNRGOV et la manière dont il est utilisé peuvent varier en fonction des législations nationales et des accords entre les compagnies aériennes et les autorités gouvernementales.

§ 2 – Le multilatéralisme européen comme instrument de référence en matière d’harmonisation

Le continent européen a été le théâtre de deux guerres mondiales dévastatrices au cours du XX^e siècle. La Seconde Guerre mondiale, en particulier, a laissé des pays ravagés et épuisés. La nécessité de prévenir de futurs conflits armés a été un moteur essentiel de la création des Communautés européennes, ancêtres de l’Union européenne, visant à favoriser la coopération économique, politique et culturelle pour éviter de nouvelles guerres entre les États européens¹⁷²⁸. Après la fin des hostilités en 1945, de nombreux dirigeants européens ont reconnu le besoin de renforcer la coopération économique pour promouvoir la prospérité et la stabilité. Le plan Marshall¹⁷²⁹, qui a fourni une aide économique importante aux États européens dévastés, a joué un rôle primordial dans la promotion de cette coopération économique.

La création de l’Union européenne a également été motivée par l’aspiration à promouvoir les droits de l’Homme, la démocratie et les valeurs communes en Europe. En effet, après les atrocités de la Seconde Guerre mondiale, de nombreux chefs d’États européens ont cherché à jeter les bases d’une structure politique qui garantirait la primauté du droit et des principes démocratiques. Le Traité de Rome de 1957¹⁷³⁰ a jeté les bases de la création d’un marché commun européen visant à éliminer les barrières tarifaires et non-tarifaires entre les pays membres. Cette coopération économique s’est donné pour objectif de favoriser la croissance économique et la prospérité mutuelle. Au fil des années, d’autres pays européens ont manifesté leur intérêt pour rejoindre la Communauté économique européenne (CEE), prédécesseur de l’Union européenne. L’élargissement de l’UE à de nouveaux membres a contribué à consolider la paix, la stabilité et la coopération à travers le continent.

¹⁷²⁸ P. FONTAINE, *L’Union européenne : Histoire, institutions, politiques*, Points, 3 mai 2012.

¹⁷²⁹ G. DE MÉNIL, « L’importance historique du plan Marshall », *Commentaire*, 2022/2, n° 178, 2022.

¹⁷³⁰ Traité de Rome, Traité instituant la Communauté économique européenne (CEE), 25 mars 1957. Voir : C. WIHTOL DE WENDEN, J. DRAVIGNY, « Soixante ans après le Traité de Rome : regards sur la liberté de circulation en Europe », *Migrations société*, 2019, pp. 17-29.

De cette construction politico-économique est né un multilatéralisme européen¹⁷³¹, une approche adoptée par les États membres pour résoudre les défis mondiaux et régionaux en favorisant la coopération et la coordination entre différents acteurs internationaux et en mettant l'accent sur la négociation multilatérale, la diplomatie ainsi que la recherche de solutions communes par le biais de forums et d'organisations internationales. Ce multilatéralisme européen repose sur le respect du droit international et la promotion des traités et accords internationaux en tant que bases d'un ordre international fondé sur des règles pour résoudre les conflits et relever les défis mondiaux.

C'est dans ce contexte que la directive (UE) 2016/681¹⁷³² relative à la collecte et l'utilisation des données des passagers aériens pour les vols internationaux a été élaborée. Ce texte a été adopté dans le but de renforcer la sécurité intérieure et la lutte contre le terrorisme en permettant aux autorités compétentes de recueillir et d'analyser les informations relatives aux passagers tout en prévoyant des mesures pour les protéger, notamment en posant des règles de sécurité strictes et en limitant l'accès à l'information.

Cette directive a été prise en réponse aux défis sécuritaires croissants qui se posent aux différents États, plus particulièrement aux États membres européens. En effet, au fil des années la menace terroriste est devenue une préoccupation majeure pour les gouvernements européens, notamment après les attaques de Madrid en 2004, de Londres en 2005 et surtout de Paris en 2015¹⁷³³. Cette dernière attaque terroriste a encouragé tous les États membres européens à aller vers l'élaboration d'une directive PNR qui permettrait notamment de faire face aux défis posés par le retour des combattants étrangers¹⁷³⁴ et les autres menaces d'infractions terroristes.

Le 17 février 2021, la Commission et le Haut représentant ont présenté, dans un communiqué de presse, leur stratégie « destinée à renforcer la contribution de l'UE à un multilatéralisme

¹⁷³¹ G. JOFFÉ, "European multilateralism and soft power projection in the Mediterranean", Instituto da Defesa Nacional, 2 series, n° 101, Primavera 2002, en ligne à URL : https://comum.rcaap.pt/bitstream/10400.26/1336/1/NeD101_GeorgeJoffe.pdf consulté le 10 août 2023.

¹⁷³² 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.

¹⁷³³ G. REILHAC, « Feu vert du Parlement européen à la collecte des données PNR », *Reuters*, Sociétés, 14 avril 2016, en ligne à URL : <https://www.reuters.com/article/union-parlement-pnr-idFRL5N17H2Q0> consulté le 10 août 2023.

¹⁷³⁴ Parlement européen, "The proposed EU passenger namerecords (PNR) directive, Revived in the new security context", Briefing, avril 2015, en ligne à URL : <https://www.europarl.europa.eu/EPRS/EPRS-Briefing-554215-The-EU-PNR-Proposal-FINAL.pdf> consulté le 10 août 2023.

fondé sur des règles »¹⁷³⁵. Cette communication a permis de partager les attentes et les ambitions des institutions européennes pour le système multilatéral. La proposition suggère d'utiliser tous les outils dont dispose l'Union européenne, aussi bien politique, diplomatique que financier, pour promouvoir les droits de l'Homme, la démocratie et le droit international dans le monde.

Pour la Commission, cette proposition s'explique par le contexte du XXI^e siècle qui nécessite une « gouvernance multilatérale accrue, et non réduite, ainsi qu'une coopération internationale fondée sur des règles »¹⁷³⁶. En effet, l'Union européenne semble considérer qu'il existe aujourd'hui des priorités stratégiques dans des domaines qu'aucun pays ne peut gérer seul, qu'il s'agisse de la paix, de la sécurité, des droits de l'Homme et de l'État de droit, du développement durable, de la santé publique ou du climat. Par conséquent, ces sujets doivent avoir prioritairement été discutés au niveau multilatéral dans le cadre d'une approche stratégique pour assurer un monde plus sûr et une coopération mondiale durable et inclusive.

L'Union européenne appelle de ses vœux une modernisation du système multilatéral qui doit, par exemple, encourager la modernisation d'institutions internationales comme l'OMS et initier l'élaboration de nouvelles organisations mondiales ainsi que la mise en place de plateformes de coopération dans différents domaines tel l'environnement numérique¹⁷³⁷. Dans ce contexte, la modernisation du système multilatéral européen peut jouer un rôle primordial dans l'amélioration et le renforcement du système PNR en Europe, voire dans le monde. Tout d'abord, elle peut encourager une meilleure harmonisation des législations en matière de collecte et d'utilisation des données PNR en renforçant la coopération entre les institutions et l'UIP (Unité Information Passagers) qui sont investis dans ce domaine.

Ensuite, une meilleure coopération multilatérale peut faciliter le partage d'expertise et d'information entre les États membres et ainsi aider au développement de meilleures pratiques en matière de protection de données personnelles des passagers aériens, notamment d'un point de vue juridique et de protection des systèmes d'information. Aussi, une modernisation du cadre multilatéral européen peut aider à renforcer la capacité des pays européens à lutter contre la criminalité transfrontalière et le terrorisme, en encourageant le partage efficace et rapide d'informations entre les États membres.

¹⁷³⁵ Commission européenne, « Un multilatéralisme renouvelé, adapté au 21^e siècle: le programme de l'UE », Communiqué de presse, 17 février 2021, Bruxelles, en ligné à URL : https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_622 consulté le 13 août 2023.

¹⁷³⁶ Ibidem

¹⁷³⁷ Ibid.

Enfin, un environnement multilatéral moderne permet au système PNR d'être utilisé dans le cadre d'accords internationaux entre l'Union européenne et d'autres pays. Une modernisation du système multilatéral faciliterait la négociation et la mise en œuvre de ces accords en créant un cadre juridique uniforme, clair et efficace.

En conclusion, la modernisation du système multilatéral européen peut être l'occasion d'améliorer et de renforcer le cadre juridique du système PNR européen. Cela pourrait conduire à une meilleure coordination, à une plus grande efficacité dans la lutte contre la criminalité et le terrorisme et à une meilleure protection des droits fondamentaux des citoyens européens, notamment du droit à la protection des données à caractère personnel et le droit à la vie privée.

§ 3 – Le bilatéralisme comme mode privilégié d'encadrement des échanges des données des passagers aériens

Le bilatéralisme¹⁷³⁸ apparaît au XIX^e siècle, au moment où les relations commerciales internationales prenaient leur plein essor. Ce mouvement trouve son vecteur juridique dans la convention bilatérale, un acte consensuel passé en la forme écrite par deux États, destiné à produire des effets de droit et régi par le droit international, selon la Convention de Vienne du 23 mai 1969 sur le droit des traités¹⁷³⁹. Historiquement, les traités de commerce et les accords de commerce sont les deux instruments bilatéraux les plus développés, ceux-ci ayant joué un rôle important en droit international commercial.

Depuis le début du XXI^e siècle, on constate une résurgence d'un certain bilatéralisme qui trouve son origine dans l'enlisement des négociations multilatérales dans le cadre de l'OMC, notamment durant le cycle de Doha¹⁷⁴⁰. Les accords bilatéraux ont proliféré, dépassant les domaines couverts par l'OMC et créant des flux d'échanges préférentiels entre les pays membres. Les principaux acteurs de cette nouvelle approche sont l'Union européenne, les États-Unis et certains pays d'Asie du Sud-Est, dont la Chine et le Japon, qui étaient jadis réticents vis-à-vis de ce type d'accords.

Le bilatéralisme peut servir de laboratoire d'essai du multilatéralisme. Dans certains cas les accords bilatéraux sont les initiateurs d'autres accords ; ils sont condamnés à s'élargir soit

¹⁷³⁸ D. CARREAU, P. JUILLARD, « Négociations commerciales internationales », *Répertoire de droit international*, Dalloz, août 2017.

¹⁷³⁹ Convention de Vienne sur le droit des traités, 23 mai 1969, Vienne, en ligne à URL : https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXIII-1&chapter=23&Temp=mtdsg3&clang=fr consulté le 13 août 2023.

¹⁷⁴⁰ V. HEYDON, WOODCOCK, *The rise of bilateralism: comparing American, European and Asian approaches to preferential trade agreements*, UN University Press, 2009.

pour se dissoudre dans un semble plus structuré, soit parce qu'il est difficile aux États concernés de ne pas ouvrir d'autres les avantages qu'ils s'offrent, comme dans le cas des accords de défense nationale¹⁷⁴¹. Dans d'autres cas, les perspectives de transformation du cadre juridique sont plus ou moins annoncées dès le départ. Ainsi, aux États-Unis, il existe depuis 1930 une tradition qui se manifeste par la conclusion d'accords bilatéraux pour la libéralisation des échanges, comme l'Accord de libre-échange (ALE) entre les États-Unis et le Canada. Cet accord bilatéral a jeté les bases d'un accord multilatéral, l'Accord de libre-échange nord-américain (ALENA)¹⁷⁴².

Une dynamique similaire peut être trouvée dans le développement des actes juridiques encadrant le traitement et le transfert des données des dossiers passagers puisque les premiers accords en la matière étaient bilatéraux, notamment le premier accord entre l'Union européenne et les États-Unis dès 2007. Depuis, les accords bilatéraux se sont multipliés entre l'Union européenne et d'autres pays comme le Canada ou l'Australie. Dix ans plus tard, une directive européenne est venue encadrer le transfert de ces données aux autorités répressives des États membres et leur traitement aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité ainsi que des enquêtes et des poursuites en la matière¹⁷⁴³.

Les accords bilatéraux ont ainsi joué un rôle significatif dans le développement et le renforcement du cadre juridique du système PNR en contribuant à établir des normes pour la collecte, l'utilisation, le transfert et la protection des données des dossiers passagers, bien qu'ils aient dû être révisés plusieurs fois sous la pression – positive et efficace – des institutions européennes, notamment de la CJUE¹⁷⁴⁴. Les accords bilatéraux peuvent également influencer les négociations d'accords multilatéraux ou d'accords au sein de l'Union européenne, ce qui fut le cas avec la directive PNR. Aussi, les accords bilatéraux dans le domaine du PNR renforcent la coopération entre les pays en matière de lutte contre la criminalité transfrontalière et le terrorisme. Ils facilitent le partage d'informations entre les autorités compétentes, ce qui peut améliorer l'efficacité de la détection et de la prévention des

¹⁷⁴¹ C. BRÉCHON-MOULÈNES, « Marchés publics », *Répertoire de droit international*, Dalloz, mars 2009.

¹⁷⁴² Ibidem

¹⁷⁴³ Europa, « Directive de l'UE relative aux données des dossiers passagers (PNR) », Conseil européen, Action de l'UE face au terrorisme, 31 août 2022, en ligne à URL : [https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/passenger-name-record/#:~:text=La%20directive%20PNR%20r%C3%A9glemente%20le,des%20poursuites%20en%20la%20mat%C3%A8re](https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/passenger-name-record/#:~:text=La%20directive%20PNR%20r%C3%A9glemente%20le,des%20poursuites%20en%20la%20mat%C3%A8re,consulté le 13 août 2023), consulté le 13 août 2023.

¹⁷⁴⁴ CJUE, « La Cour déclare que l'accord sur le transfert des données des dossiers passagers, prévu entre l'Union européenne et le Canada, ne peut être conclu sous sa forme actuelle », Communiqué de presse, n° 84/17, Avis 1/15, Luxembourg, 26 juillet 2017, en ligne à URL : <https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084fr.pdf> consulté le 14 août 2023.

menaces ; toutefois, cela nécessite des dispositions spécifiques visant à protéger les droits et la vie privée des citoyens et des passagers aériens. Les institutions européennes ont ainsi exigé des garanties et envisagé des mécanismes de recours en cas d'atteinte aux droits fondamentaux des passagers aériens¹⁷⁴⁵.

Sous-section 2 – Les législations des dossiers passagers au défi de l'harmonisation

L'harmonisation des législations est un défi en raison de plusieurs facteurs complexes et souvent interdépendants. Les négociations visant à harmoniser les lois sur des sujets tels que les droits fondamentaux peuvent être compliquées en raison de leurs implications multiples d'un point de vue politique et social. Aussi, les politiques nationales et les intérêts nationaux peuvent diverger. Certains pays peuvent être réticents à harmoniser leurs lois si cela va à l'encontre de leurs objectifs nationaux ou de leurs priorités politiques.

§ 1 – Une interaction mitigée entre multilatéralisme et unilatéralisme source de défis pour l'harmonisation des législations des dossiers passagers

L'harmonisation du cadre juridique des dossiers passagers au niveau international, régional et national peut être complexe en raison de diverses raisons. Les pays ont des législations différentes en matière de protection des données à caractère personnel et harmoniser ces règles divergentes pour élaborer un cadre cohérent et efficace peut être difficile, certains pays pouvant disposer de règles plus souples en matière de protection des droits fondamentaux. La collecte et le traitement des données PNR peuvent entraîner des préoccupations en matière de droits de l'Homme et de vie privée. L'harmonisation doit tenir compte de ces préoccupations et établir des garanties solides pour protéger les droits individuels. Les perspectives culturelles¹⁷⁴⁶, philosophiques et politiques des différents pays peuvent influencer la manière dont le législateur aborde le traitement et la protection des données à caractère personnel. Les définitions et termes juridiques peuvent varier d'un continent à un autre, d'un pays à un autre. C'est pourquoi l'harmonisation nécessite d'unifier et de clarifier ces termes afin d'éviter les interprétations et les ambiguïtés erronées. Par ailleurs, le développement des technologies numériques de manière rapide peut rendre obsolètes les cadres juridiques existants. L'harmonisation doit être conçue de façon flexible afin de s'adapter activement aux nouvelles

¹⁷⁴⁵ S. PEYROU, « Accord PNR UE-Canada : validation par la CJUE du système PNR, des modalités à revoir ! (réflexions sur l'avis 1/15 de la CJUE, 26 juillet 2017) », *GDR ELSJ*, 28 juillet 2017, en ligne à URL : <http://www.gdr-elsj.eu/2017/07/28/informations-generales/accord-pnr-ue-canada-validation-cjue-systeme-pnr-modalites-a-revoir-reflexions-lavis-115-de-cjue-26-juillet-2017/> consulté le 14 août 2023.

¹⁷⁴⁶ Y. SENECHAL, P. NOREAU, « Présentation : prolégomènes à une sociologie des cultures juridiques », *Sociologie et sociétés*, 52(2), 2020, pp. 13-38, en ligne à URL : <https://id.erudit.org/iderudit/1088748ar> consulté le 14 août 2023.

technologies et systèmes d'information pour avoir des systèmes PNR efficaces et protégeant efficacement les données personnelles des passagers aériens.

Une sorte de dynamique par ricochet du cadre multilatéral peut créer, à son tour, un environnement juridique favorable au développement du bilatéralisme. Mises à part quelques exceptions, comme l'hypothèse des financements par la Banque mondiale, le multilatéralisme à l'état pur est loin d'exister. Par exemple, l'Accord plurilatéral sur les marchés publics de l'OMC n'a été signé que par une douzaine de membres, dont l'Union européenne ; qui plus est, en raison de la technique des panels, il s'agit, d'une certaine façon, un ensemble d'accords bilatéraux. D'ailleurs, le multilatéralisme comme celui qui se développe sous l'égide de l'OMC, n'est pas nécessairement souhaitable. Tous les États ne peuvent pas nécessairement avoir la même situation. Cette comparaison permet de comprendre les défis qui se posent pour la protection des données personnelles. Il faudrait peut-être aussi de nouvelles organisations dédiées à la protection des données à caractère personnel ou, plus modestement, privilégier le régionalisme qui a le mérite de favoriser les solidarités de proximité et la volonté de coopération au-delà des rivalités ou des appréhensions passées. La solution n'est pas évidente tant les non-dits pèsent lourds dans la manière d'appréhender les défis du droit des nouvelles technologies.

Les défis politico-juridiques peuvent également entraîner des conséquences négatives pour l'harmonisation des législations des dossiers passagers dans le contexte actuel où la primauté du droit européen, et même l'État de droit, est remise en cause par certains gouvernements européens. C'est le cas de la Hongrie¹⁷⁴⁷, État membre de l'Union européenne, dont certains actes ont suscité des inquiétudes en raison des préoccupations des autres États membres concernant les valeurs démocratiques et l'État de droit. En effet, certaines décisions du Gouvernement hongrois, notamment des réformes judiciaires contestées, ont soulevé des interrogations quant à au respect des principaux fondamentaux de l'Union européenne. Ces décisions ont été critiquées pour leur potentiel à limiter l'indépendance des juges.

Or, ces préoccupations peuvent affecter l'harmonie au sein des États membres européens. Outre les désaccords entre États membres eux-mêmes, ces séquences peuvent entraîner des tensions avec les institutions européennes elles-mêmes. Les désaccords sur les valeurs démocratiques et les principes fondamentaux peuvent compromettre la confiance mutuelle nécessaire à la coopération dans le cadre de la vie de l'Union.

¹⁷⁴⁷ AFP, « Hongrie : cinquième jour de manifestations contre une réforme d'Orban », *Le Figaro*, 17 juillet 2022, en ligne à URL : <https://www.lefigaro.fr/flash-eco/hongrie-cinquieme-jour-de-manifestations-contre-une-reforme-d-orban-20220717> consulté le 17 août 2023.

Il existe alors une crainte de fragmentation des lois et des décisions au sein d'une Union européenne à deux vitesses, certains pays pouvant avancer l'intégration plus rapidement que d'autres dans certains domaines. En général, cela se produit en raison de différences de priorités nationales ou de développements économiques ou d'opinions sur tel secteur. Au sein de l'Union européenne, cette possibilité permet à certains pays de former des alliances plus étroites pour poursuivre des objectifs communs tandis que d'autres États membres peuvent choisir d'avancer à un rythme différent. Si au sein de l'Union européenne, les institutions s'efforcent en principe de maintenir la cohésion et l'unité entre tous les États, dans d'autres scénarios, on peut craindre une fragmentation du cadre juridique avec différents niveaux de coopération sur un sujet. C'est la crainte dans le domaine du droit des dossiers passagers où les accords de transfert des dossiers passagers, et leur protection, s'effectue sur certains axes précis seulement, à savoir entre l'Union européenne et d'autres États partageant ses valeurs et sa conception du droit comme les États-Unis ou l'Australie.

La fragmentation provient parfois d'un État qui décide d'initier le développement d'une relation bilatérale avec un autre État sans se soucier des préoccupations de ses partenaires avec lesquels il est pourtant lié par un accord ou un Traité de droit international. L'unilatéralisme de l'Italie dans sa relation avec la Chine a par exemple été critiqué par ses partenaires européens, car l'action du Gouvernement italien ne prenait pas en compte les dynamiques géopolitiques, économiques et stratégiques européennes¹⁷⁴⁸. L'unilatéralisme ici se développe contre un cadre multilatéral, qu'il affaiblit. En effet, l'Italie a signé en 2019 un protocole d'accord¹⁷⁴⁹ pour rejoindre l'initiative chinoise *Belt and Road Initiative*¹⁷⁵⁰. Annoncée comme l'un des plus grands projets d'infrastructure de l'histoire, la « nouvelle route de la Soie » vise à accroître la coopération et la connectivité de la région eurasiatique à travers principalement des infrastructures et des accords commerciaux¹⁷⁵¹. Le renouvellement du projet d'accord, prévu pour 2024, n'a pas eu lieu parce que l'Italie s'est retirée du

¹⁷⁴⁸ F. MASELLI, « Le casse-tête chinois de Meloni : enquête au cœur de l'Italie des Nouvelles Routes de la soie », *Le Grand Continent*, 9 juillet 2023, en ligne à URL : <https://legrandcontinent.eu/fr/2023/07/09/le-casse-tete-chinois-de-meloni-enquete-au-coeur-de-litalie-des-nouvelles-routes-de-la-soie/> consulté le 21 août 2023.

¹⁷⁴⁹ Ministère des Affaires Étrangères de la République Populaire de Chine et Ministère des Affaires Étrangères et de la Coopération Internationale de la République Italienne, « Memorandum d'accord entre le gouvernement de la République populaire de Chine et le gouvernement de la République italienne sur la coopération dans le cadre de l'initiative de la ceinture et de la route », signé le 23 mars 2019.

¹⁷⁵⁰ Belt and Road Initiative est un programme de développement des infrastructures à l'échelle mondiale adoptée par le gouvernement chinois en 2013 pour investir dans plus de 150 pays et organisations internationales. Voir en ce sens : J. MCBRIDE, N. BERMAN, A. CHATZKY, « China's Massive Belt and Road Initiative », *Council on Foreign Relations*, 2 février 2023, en ligne à URL : <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative> consulté le 30 août 2024.

¹⁷⁵¹ S. TENENBAUM, « Belt And Road Initiative : Quels enjeux pour la Chine et ses partenaires ? », *BSI Economics*, 12 mars 2019, en ligne à URL : <https://www.bsi-economics.org/977-belt-road-initiative-enjeux-chine-partenaires-st> consulté le 21 août 2023.

programme *Belt and Road Initiative*¹⁷⁵². Toutefois, les deux pays ont signé un plan d'action en juillet 2024¹⁷⁵³ pour renforcer leur relation bilatérale. La participation italienne avait soulevé beaucoup de controverses, notamment du fait que c'est l'un des seuls pays du G7 à avoir accepté ce choix diplomatique qui étend l'influence chinoise. La Chine a intensifié ses efforts pour élargir son influence en Europe et partout dans le monde en investissant dans des projets d'infrastructure, en établissant des partenariats économiques et en cherchant à renforcer les liens politiques. Certains États, dont ceux de l'Union européenne, pourraient craindre que des relations bilatérales étroites avec la Chine ne fassent partie d'une stratégie plus large visant à exercer une influence politique et économique en Europe.

Or, les pays européens préfèrent en général coordonner leurs politiques et actions vis-à-vis de partenaires étrangères, notamment de puissances mondiales concurrentes comme la Chine¹⁷⁵⁴. Lorsqu'un pays comme l'Italie prend des décisions unilatérales dans le cadre de ses relations bilatérales avec la Chine, cela peut être perçu comme un affaiblissement de la position commune de l'Union enfreinant, par conséquent, la solidarité européenne.

De plus, les pays de l'Union européenne peuvent avoir des préoccupations en matière de sécurité en ce qui concerne les relations étroites entre certains États membres et la Chine¹⁷⁵⁵. Les partenariats économiques et technologiques avec la Chine peuvent potentiellement avoir des implications en matière de sécurité, notamment en ce qui concerne la protection des données à caractère personnel, la technologie de pointe et la souveraineté numérique. En effet, les relations de l'Union européenne avec la Chine sont souvent traversées par des préoccupations concernant les droits de l'Homme, notamment en ce qui concerne les questions de liberté d'expression, de répression politique et de traitement des minorités. Certains pays européens, comme l'Allemagne et la France¹⁷⁵⁶, ont critiqué ces initiatives qui

¹⁷⁵² C. BROADHURST, « En visite en Chine, la Première ministre italienne Giorgia Meloni cherche à relancer les relations », *RFI*, publié le 29 juillet 2024, en ligne à URL : <https://www.rfi.fr/fr/asie-pacifique/20240729-en-visite-en-chine-la-premi%C3%A8re-ministre-italienne-giorgia-meloni-cherche-%C3%A0-relancer-les-relations> consulté le 30 août 2024.

¹⁷⁵³ Italie et Chine, « Plan d'action triennal pour la mise en œuvre des accords bilatéraux et l'exploration de nouvelles pistes de coopération », signé le 28 juillet 2024.

¹⁷⁵⁴ J. LIBOREIRO, « Les six principaux points de friction entre l'UE et la Chine », *Euronews*, 3 avril 2023, en ligne à URL : <https://fr.euronews.com/my-europe/2023/04/03/les-six-principaux-points-de-friction-entre-lue-et-la-chine> consulté le 21 août 2023.

¹⁷⁵⁵ Commission européenne, « Discours de la Présidente von der Leyen sur les relations UE - Chine à l'intention du Mercator Institute for China Studies et du Centre de politique européenne », Discours, 30 mars 2023, en ligne à URL : https://france.representation.ec.europa.eu/informations/discours-de-la-presidente-von-der-leyen-sur-les-relations-ue-chine-lintention-du-mercator-institute-2023-03-30_fr consulté le 21 août 2023.

¹⁷⁵⁶ *Le Monde*, « L'Italie rejoint les « nouvelles routes de la soie » de la Chine », 23 mars 2019, en ligne à URL : https://www.lemonde.fr/economie/article/2019/03/23/malgre-l-inquietude-de-bruxelles-l-italie-rejoint-les-nouvelles-routes-de-la-soie-de-pekine_5440367_3234.html consulté le 30 août 2024.

semblent privilégier les intérêts économiques aux dépens des préoccupations politiques et sécuritaires.

En fin de compte, les critiques envers l'unilatéralisme de l'Italie dans ses relations avec la Chine reflètent souvent des préoccupations plus larges liées à la coordination européenne, à la sécurité, à l'influence étrangère et à la préservation des valeurs européennes communes, comme la protection des droits fondamentaux ; elles peuvent aussi concerner le droit à la protection des données à caractère personnel.

Cette érosion de la concertation entre les acteurs d'un même ensemble politique peut entraîner des conséquences sur l'architecture juridique du cadre multilatéral que ces derniers ont mis en place. Ces tendances peuvent avoir un effet négatif sur l'harmonisation des législations nationales, notamment sur le transfert et la protection des données des passagers aériens (PNR), car le monde actuel est passé de la compétition à la confrontation¹⁷⁵⁷ et cela n'aide pas à l'harmonisation souhaitée des législations qui implique une volonté des États de converger vers un accord international réunissant une majeure partie des États membres des Nations unies.

§ 2 – Un déséquilibre dans les rapports de forces entre Européens et Américains comme obstacle à l'harmonisation du droit des dossiers passagers

Depuis le début du XXI^e siècle, la relation euro-américaine a joué un rôle primordial dans la construction du droit encadrant les données des dossiers passagers (PNR), notamment en initiant le premier accord sur le transfert et le traitement de ces données. Après les attentats du 11 septembre 2001, la coopération internationale en matière de sécurité aérienne est devenue une priorité ; le Gouvernement américain a obligé les compagnies aériennes à fournir ces données pour pouvoir laisser attirer les avions sur son sol. Les États-Unis et l'Union européenne ont rapidement reconnu la nécessité de partager des informations sur les passagers afin de prévenir les menaces terroristes tout en essayant de protéger les données des passagers aériens. Cette première coopération a été un facteur clé de la construction du droit PNR. Les États-Unis ont conclu des accords bilatéraux avec plusieurs pays européens pour mettre en

¹⁷⁵⁷ R. GUBERT, B. ESCHAPASSE, « DGSE : « Nous avons la clandestinité en héritage », *Le Point*, International, Entretien avec le patron de la DGSE Bernard Émié, 28 juin 2023, en ligne à URL : https://www.lepoint.fr/monde/dgse-nous-avons-la-clandestinite-en-heritage-28-06-2023-2526465_24.php#11 consulté le 21 août 2023.

place le partage de données PNR¹⁷⁵⁸. Ces accords ont servi de modèle aux négociations multilatérales entre l'Union européenne et les États-Unis.

Cette construction n'a pas été un long fleuve tranquille. En effet, les débats entre l'Union européenne et les États-Unis ont porté sur la manière dont les données PNR devraient être collectées, utilisées et protégées¹⁷⁵⁹. Ces discussions ont abouti à la définition de normes et de garanties minimales pour s'assurer que les données des passagers aériens soient traitées de manière sécurisée et respectueuse de la vie privée en répondant aux standards élevés de l'Union européenne.

La difficulté dans les négociations entre les deux parties a notamment porté sur la manière de parvenir à un équilibre entre la protection des droits individuels et la nécessité de garantir la sécurité collective. Des préoccupations juridiques ont été soulevées par les associations de défense des droits de l'Homme¹⁷⁶⁰ concernant la collecte et l'utilisation des données PNR. Les questions liées à la protection des droits fondamentaux ont parfois été traitées devant les tribunaux¹⁷⁶¹, ce qui a influencé la façon dont les autres accords PNR ont été formulés, notamment l'accord PNR entre le Canada et l'Union européenne¹⁷⁶².

Ainsi, la relation juridique euro-américaine a initié la construction du droit PNR à travers des accords bilatéraux, des négociations multilatérales et des discussions sur l'équilibre entre la sécurité et la protection des données. C'était aussi le début de l'harmonisation d'une nouvelle architecture juridique autour des données des dossiers passagers qui a commencé avec le premier accord PNR euro-américain, s'est consolidée avec la directive européenne sur le PNR, et peut-être poursuivie avec l'accord PNR euro-japonais¹⁷⁶³. Cette multiplication

¹⁷⁵⁸ À cet égard, on peut citer l'accord entre le gouvernement américain et le gouvernement tchèque. Ministry of the Interior of the Czech Republic and Department of Homeland Security of the United States of America, "Memorandum of Understanding Regarding the United States Visa Waiver Program and Related Enhanced Security Measures", 2008.

¹⁷⁵⁹ Eur-Lex, « Accord entre l'Union européenne et les États-Unis concernant les données des dossiers des passagers aériens », 26 août 2021, en ligne à URL : <https://eur-lex.europa.eu/FR/legal-content/summary/eu-us-agreement-on-airline-passenger-name-record-data.html> consulté le 21 août 2023.

¹⁷⁶⁰ Ligue des droits de l'Homme, « Nouvel accord PNR (UE-USA) : Pas d'amélioration, le PE doit le rejeter ! », données personnelles, 25 janvier 2012, en ligne à URL : <https://www.ldh-france.org/Nouvel-accord-PNR-UE-USA-pas-d/> consulté le 21 août 2023.

¹⁷⁶¹ C'est le cas dans les affaires jugées par la CJUE : Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a., CJUE, Affaires jointes C-293/12 et C-594/12, 8 avril 2014 et Maximilian Schrems c/ Data Protection Commissioner, affaire C-362/14, 6 octobre 2015.

¹⁷⁶² S. PEYROU, « Accord PNR UE-Canada : validation par la CJUE du système PNR, des modalités à revoir ! », GDR-ELSJ, 28 juillet 2017, en ligne à URL : <http://www.gdr-elsj.eu/2017/07/28/informations-generales/accord-pnr-ue-canada-validation-cjue-systeme-pnr-modalites-a-revoir-reflexions-lavis-115-de-cjue-26-juillet-2017/> consulté le 21 août 2023.

¹⁷⁶³ Conseil de l'UE, « Accord PNR entre l'UE et le Japon: le Conseil autorise l'ouverture de négociations », Communiqué de presse, 18 février 2020, en ligne à URL : <https://www.consilium.europa.eu/fr/press/press->

d'accords bilatéraux et d'actes juridiques européens pourrait permettre de faire converger les points de vue des États de l'Organisation des Nations-Unies en vue de l'élaboration d'un traité international relatif au transfert, au traitement et à la protection des données des dossiers passagers.

Une perte d'équilibre dans cette relation euro-américaine originelle en matière de PNR ou une crise de confiance pourrait avoir un effet négatif sur le futur de l'harmonisation des législations relatives aux dossiers passagers, notamment si les deux parties n'arrivent plus à faire converger leurs intérêts et leurs points de vue.

Le renouvellement de la loi sur l'espionnage aux États-Unis, plus précisément l'article 702 du Foreign Intelligence Surveillance Act qui permet aux renseignements américains d'intercepter les communications entre étrangers et citoyens américains¹⁷⁶⁴ au nom de la lutte contre le terrorisme, a fait l'objet de divers débats aux États-Unis et au-delà. Pour le juriste Max Schrems¹⁷⁶⁵, ce renouvellement de la loi aurait dû être une occasion pour les gouvernements européens d'imposer plus de garanties de protection pour les données personnelles de leurs citoyens qui jusqu'à aujourd'hui sont massivement accessibles aux agences fédérales de renseignement. Cette section 702 permet notamment aux autorités américaines d'avoir accès aux appels téléphoniques et aux courriels des individus résidant à l'étranger.

Aux États-Unis, cette disposition a été critiquée pour son utilisation au-delà de son objet initial, car la loi se serait transformée en un outil d'espionnage des citoyens américains et pas seulement des étrangers, au grand dam des associations de défense des droits de l'Homme¹⁷⁶⁶. Dans l'espace de l'Union européenne, c'est ce même texte qui est à l'origine de l'annulation par la CJUE de l'accord transatlantique sur les données vers États-Unis, en juillet 2020, après le recours initié par Max Schrems et son association Not of your business (NOYB)¹⁷⁶⁷.

Il était en l'espèce reproché à la législation américaine d'autoriser un accès massif et sans distinction aux données personnelles des Européens, sans fournir les « garanties

[releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/](https://www.intelligenceonline.fr/renseignement-d-etat/2023/04/27/les-cartels-mexicains-a-la-rescousse-involontaire-de-la-prolongation-de-l-article-702-sur-les-interceptions,109948918-art) consulté le 21 août 2023.

¹⁷⁶⁴ Intelligence Online, « Les cartels mexicains à la rescousse (involontaire) de la prolongation de l'article 702 sur les interceptions », États-Unis, 27 avril 2023, en ligne à URL : <https://www.intelligenceonline.fr/renseignement-d-etat/2023/04/27/les-cartels-mexicains-a-la-rescousse-involontaire-de-la-prolongation-de-l-article-702-sur-les-interceptions,109948918-art> consulté le 22 août 2023.

¹⁷⁶⁵ S. BASCOU, « Comment l'Europe a abandonné vos données personnelles aux espions américains », *01net*, Politique, Droits, 2 juillet 2023, en ligne à URL : <https://www.01net.com/actualites/comment-leurope-a-abandonne-vos-donnees-personnelles-aux-espions-americains.html> consulté le 22 août 2023.

¹⁷⁶⁶ Human Rights Watch, « Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act », 14 septembre 2017, en ligne à URL : <https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance> consulté le 22 août 2023.

¹⁷⁶⁷ S. BASCOU, op. cit.

suffisantes »¹⁷⁶⁸ de protection telles que prévues par le RGPD, à savoir le contrôle d'un juge lorsque les données sont consultées et une information préalable. Or, les débats aux États-Unis n'ont pas mentionné les droits des Européens, car la loi en question distingue les citoyens américains qui disposent de droits, comme le contrôle par le juge de l'écoute, et les ressortissants, qui selon Max Schrems ne disposent pas de droits¹⁷⁶⁹.

Par ailleurs, les arrêts du juge européen invalidant le « Safe Harbor » en 2015 puis le « Privacy Shield » en juillet 2020 n'ont pas produit de grands changements dans l'effort de trouver un compromis entre les législations américaines et européennes étant donné que les entreprises qui transfèrent les données des Européens vers le sol américain ont continué de le faire en invoquant des solutions juridiques alternatives¹⁷⁷⁰ pour poursuivre ces transferts, dont la légalité n'est pas certaine selon Max Schrems.

La guerre en Ukraine est ensuite venue bouleverser ce rapport de force. Un nouvel accord entre Européens et Américains a été annoncé par la Présidente de la Commission européenne et le Président américain le 25 mars 2022¹⁷⁷¹. Celui-ci aspire à remédier aux travers des deux premiers accords en prévoyant un mécanisme de recours pour les citoyens européens devant un officier de la direction du renseignement américain ou d'un tribunal indépendant formé par le ministère de la Justice américaine et une limitation de l'accès aux données aux « objectifs de sécurité nationale »¹⁷⁷². Cet accord (« Privacy Shield ») a été critiqué par le Parlement européen et les CNIL européennes. Pour Max Schrems, il s'agissait surtout d'un accord politique échangeant les données personnelles des Européens contre du gaz liquéfié américain dans un contexte de guerre en Ukraine, avec une protection des droits fondamentaux, notamment des données à caractère personnel et de la vie privée, marginalisée¹⁷⁷³.

L'incapacité de trouver un accord transatlantique équilibré entre Américains et Européens sur le transfert des données personnelles, comme l'a montré le « Privacy Shield », peut freiner l'harmonisation des législations sur les dossiers passagers (PNR). La divergence en matière de

¹⁷⁶⁸ Ibidem

¹⁷⁶⁹ Ibid.

¹⁷⁷⁰ Ibid.

¹⁷⁷¹ A. PIQUARD, « Europe - Etats-Unis : l'accord transatlantique controversé de transfert des données validé par Bruxelles », *Le Monde*, 10 juillet 2023, en ligne à URL : https://www.lemonde.fr/economie/article/2023/07/10/europe-etats-unis-l-accord-transatlantique-controversee-de-transfert-des-donnees-valide-par-bruxelles_6181378_3234.html consulté le 22 août 2023.

¹⁷⁷² Commission européenne, « Accord entre la Commission européenne et les États-Unis concernant le cadre transatlantique de protection des données personnelles », Représentation en France, 25 mars 2022, en ligne à URL : https://france.representation.ec.europa.eu/informations/accord-entre-la-commission-europeenne-et-les-etats-unis-concernant-le-cadre-transatlantique-de-2022-03-25_fr consulté le 22 août 2023

¹⁷⁷³ S. BASCOU, « Comment l'Europe a abandonné vos données personnelles aux espions américains », *01net*, Politique, Droits, 2 juillet 2023, en ligne à URL : <https://www.01net.com/actualites/comment-leurope-a-abandonne-vos-donnees-personnelles-aux-espions-americains.html> consulté le 22 août 2023

normes de protection constitue le premier obstacle à ce rapprochement, car les États-Unis et l'Union européenne ont des approches différentes en matière de protection des données personnelles. Les normes de protection de la vie privée et la protection des données ne sont pas alignées, ce qui peut créer des obstacles à l'harmonisation. D'où l'invalidation d'accords issue d'une préoccupation européenne concernant les pratiques de surveillance gouvernementale par les autorités américaines¹⁷⁷⁴.

L'invalidation d'un accord transatlantique crée une incertitude juridique quant à la manière dont les données à caractère personnel sont transférées d'une collectivité à une autre. Conséquemment, les entreprises qui souhaitent opérer des activités transatlantiques sont confrontées à des défis complexes pour se conformer aux législations des deux côtés de l'Atlantique, surtout dans l'Union européenne où les juridictions veillent à l'effectivité des droits. C'est dans ce contexte que la Commission irlandaise pour la protection des données (DPC) agissant pour le compte de l'Union européenne a infligé une amende de 1,2 milliard d'euros à l'encontre de la société américaine Meta, dont le siège européen est à Dublin en Irlande, au motif de la violation des règles européennes en matière de protection des données personnelles¹⁷⁷⁵.

L'absence d'accords adéquats peut placer les entreprises dans une situation difficile. En effet, celles qui traitent de données personnelles doivent s'assurer qu'elles respectent les règles de protection des données de deux espaces juridiques différents, ce qui peut entraîner une complexité administrative accrue et des coûts supplémentaires. Ainsi, l'élaboration d'accords transatlantiques nécessite des négociations et une coopération entre différents acteurs. L'invalidation d'accords existants peut créer des tensions et rendre plus difficile l'élaboration de nouveaux accords ou l'harmonisation des législations.

Aussi, les restrictions sur le transfert de données à caractère personnel peuvent entraver le commerce transatlantique et l'innovation. Les entreprises dépendent souvent de la libre circulation des données pour leurs opérations et leurs services et les restrictions peuvent entraîner des répercussions économiques négatives.

¹⁷⁷⁴ Le Figaro, « L'Union européenne adopte un nouveau cadre légal pour le transfert de données vers les États-Unis », Tech & web, 10 juillet 2023, en ligne à URL : <https://www.lefigaro.fr/secteur/high-tech/l-union-europeenne-adopte-un-nouveau-cadre-legal-pour-le-transfert-de-donnees-vers-les-etats-unis-20230710> consulté le 22 août 2023.

¹⁷⁷⁵ V. NEIRINCK-FAUVELLE, « Données personnelles : le régulateur irlandais inflige une amende record de 1,2 milliard d'euros à Meta », *Toute l'Europe*, Numérique droits fondamentaux, Revue de presse, 23 mai 2023, en ligne à URL : <https://www.touteleurope.eu/l-ue-dans-le-monde/donnees-personnelles-le-regulateur-irlandais-inflige-une-amende-record-de-12-milliard-d-euros-a-meta/> consulté le 22 août 2023

C'est dans un contexte marqué par la remise en question des accords précédents et une crise du multilatéralisme que le US-EU Data Privacy Framework, convenu entre le gouvernement américain et l'Union européenne, a été établi pour encadrer le transfert de données personnelles entre les deux parties. Ce cadre vise à assurer une protection des données conforme au Règlement général sur la protection des données (RGPD) de l'UE, garantissant ainsi un niveau de protection adéquat pour les données transférées. En conséquence, la Commission européenne a adopté une nouvelle décision d'adéquation¹⁷⁷⁶, le 10 juillet 2023, constatant un niveau de protection des données personnelles suffisant entre les États-Unis et l'Union européenne.

En somme, l'incapacité à parfaire les accords transatlantiques sur les données personnelles peut freiner l'harmonisation des législations entre Américains et Européens mais aussi avec les autres acteurs internationaux en raison des différences de normes, des préoccupations concernant la surveillance gouvernementale, de l'incertitude juridique, des contraintes pour les entreprises, ou encore des défis liés aux négociations et à la coopération entre les pays. Cela peut avoir des implications profondes sur la manière dont les données personnelles sont gérées et transférées entre les différents États du monde.

Par conséquent, la crise du multilatéralisme évoquée précédemment, caractérisée par une diminution de la coopération internationale et une remise en question des accords et institutions multilatéraux, peut avoir un impact significatif sur l'harmonisation des législations en matière de protection des données à caractère personnel entre les pays concernés. Cette crise peut affaiblir les accords conçus pour faciliter la coopération et l'harmonisation des règles entre les nations. Les accords transatlantiques sur les données personnelles en sont des exemples, visant à réglementer le transfert de données entre différents pays¹⁷⁷⁷. Si ces accords sont remis en cause ou invalidés en raison du désengagement des pays à coopérer au niveau multilatéral, cela peut entraver l'harmonisation des législations.

En l'absence de cette coopération multilatérale qui encourage un cadre général protecteur des droits fondamentaux, les pays peuvent être plus enclins à adopter des législations nationales qui reflètent leurs propres intérêts et priorités. Cela peut entraîner une fragmentation législative, avec chaque pays qui met en place ses propres normes de protection des données

¹⁷⁷⁶ Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

¹⁷⁷⁷ D. SOGGE, « La crise du multilatéralisme », Enjeux et défis du développement international : Acteurs et champs d'action. Édition nouvelle et actualisée, *Les Presses de l'Université d'Ottawa*, 2019, en ligne à URL : <https://www.jstor.org/stable/j.ctvp7d48d.19> consulté le 22 août 2023

rendant ainsi l'harmonisation des législations dans le monde encore plus difficile. Ces dynamiques ne font qu'affaiblir la protection des données personnelles des dossiers passagers (PNR) qui doivent bénéficier de standards de protection élevés partout dans le monde. Lorsque la coopération internationale diminue et que les pays se tournent vers des approches plus unilatérales, il devient plus difficile de trouver des solutions communes aux défis transnationaux telle la protection des données à caractère personnel des passagers aériens.

Conclusion de la seconde partie

La seconde partie de cette thèse nous a permis de mettre en évidence les multiples nouvelles menaces pesant sur la protection juridique des dossiers passagers (PNR). L'invasion des nouvelles technologies dans les aéroports a modifié le parcours de voyage des passagers. Cette évolution impacte davantage de manière négative les libertés publiques et individuelles. La collecte massive de données personnelles aux frontières, ainsi que le profilage des passagers, entrent en conflit avec le respect des droits fondamentaux dont la protection des données à caractère personnel. L'ingérence croissante des acteurs privés, notamment dans les aéroports, et la privatisation des aéroports aggravent cette vulnérabilité. La déterritorialisation, marquée par l'effacement du droit national dans les transferts de données personnelles, érode davantage la protection des données personnelles des passagers. En outre, la crise que vit le système multilatéral complique l'harmonisation du régime juridique des dossiers passagers dans la mesure où les crises internationales favorisent la fragmentation des législations.

CONCLUSION GÉNÉRALE

Dans cette quête permanente d'un équilibre entre la sécurité collective et la protection des droits fondamentaux, la persistance des limitations traditionnelles à la protection juridique des dossiers passagers a fait pencher la balance vers les priorités contemporaines des États, à savoir la répression des personnes susceptibles d'activités terroristes ou de crimes internationaux, tout en exprimant la volonté de mieux protéger le droit à la protection des données à caractère personnel dans les directives et traités bilatéraux d'échanges de données PNR. Il n'empêche que ces données des dossiers passagers sont vues, avant tout et surtout, comme un outil de prévention et de renseignement, contre les réseaux de grande criminalité et le terrorisme¹⁷⁷⁸. Dans ce contexte, la répression pénale n'est pas seulement privative de liberté, elle peut aussi empiéter sur les droits fondamentaux des passagers aériens¹⁷⁷⁹. En constatant l'incompatibilité de l'accord PNR conclu entre le Canada et l'Union européenne¹⁷⁸⁰ avec les droits fondamentaux garantis par les traités européens, les juges européens ont voulu assurer un niveau significatif de protection des données personnelles des passagers aériens en considérant que les droits fondamentaux des citoyens européens n'allaient pas être sacrifiés sur l'autel des impératifs sécuritaires.

Néanmoins, la préoccupation selon laquelle la logique répressive pourrait être détournée de son but initial, qui est de combattre les infractions terroristes, pour réprimer des activités politiques persiste¹⁷⁸¹. Le débat sur les conséquences des législations pénales à l'égard des droits des passagers a commencé après les attaques terroristes du 11 septembre 2001. Depuis cette date, le Gouvernement américain, en imposant aux avions atterrissant sur son sol de transmettre les données des passagers aériens, a initié une activité législative avec un caractère répressif qui domine. Les accords qui ont réuni Européens, Américains, Canadiens, Australiens et Japonais s'accordent sur l'idée de limitation des droits fondamentaux, notamment du droit à la protection des données à caractère personnel. Cette limitation s'intègre dans la stratégie européenne de lutte contre le terrorisme qui vise à « combattre le

¹⁷⁷⁸ S. SUTOUR et Y. DETRAIGNE, « Rapport n° 401 : La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives », Commission des lois, Sénat, 13 mai 2009, en ligne à URL : <http://www.senat.fr/ue/pac/E6014.html> consulté en ligne le 26 décembre 2023.

¹⁷⁷⁹ CJUE, Avis 1/15 de la Cour (grand chambre), 26 juillet 2017. En observant que l'accord était incompatible avec les droits fondamentaux protégés par les traités européens, les juges européens ont cherché à garantir une protection très élevée des données personnelles des passagers aériens. Ils ont estimé que les impératifs sécuritaires ne devaient pas conduire au sacrifice des droits fondamentaux des citoyens européens.

¹⁷⁸⁰ CJUE, Avis 1/15 de la Cour (grand chambre), 26 juillet 2017.

¹⁷⁸¹ R. KEMPF, *Ennemis d'États. Les lois scélérates des anarchistes aux terroristes*, La Fabrique éditions, 2019.

terrorisme à l'échelle mondiale et rendre l'Europe plus sûre »¹⁷⁸². Les négociations d'accords PNR se sont relevés difficiles du fait des exigences américaines en matière de transmission de données et de l'absence de contrôle démocratique, notamment de la part du Parlement européen¹⁷⁸³. Cette absence de contrôle a soulevé des inquiétudes en matière d'insécurité juridique. Elle a conduit les parlementaires européens à critiquer le niveau de protection insuffisant des données des passagers aériens, notamment en raison du manque de dispositions claires sur la conservation des données, le partage d'information et le contrôle par les autorités de protection des données. En plus du rapport de force politique avec les Américain, les accords PNR ont souffert du climat politico-juridique qui a suivi les attentats du 11 septembre 2001, caractérisé par l'affaiblissement des considérations liées aux protection des droits fondamentaux¹⁷⁸⁴.

Un *momentum* sécuritaire s'est ouvert avec les législations américaines qui obligent, via le ministère américain de la sécurité intérieure, les compagnies aériennes à transmettre les données des dossiers passagers. Toutefois, notre étude a permis de voir que l'utilisation sécuritaire des données personnelles des passagers avait déjà été pensé et appliqué aux États-Unis une décennie plus tôt. Les attentats du 11 septembre 2001 ouvrent, en fait, l'extension de cette pratique législative aux autres États du monde.

Tout en essayant de faire face à *momentum* sécuritaire, avec sa logique répressive, la directive à la prévention et la détection des infractions terroristes et formes graves de criminalité via le transfert des données passagers par les transporteurs aériens et leur traitement, en date du 27 avril 2016¹⁷⁸⁵, ne met pas fin à cette volonté américaine d'utiliser les données personnes des passagers aériens dans une démarche quasi-sécuritaire, en sacrifiant les considérations liées à la protection des données personnelles¹⁷⁸⁶. La vague d'attentats terroristes qui a touché

¹⁷⁸² Conseil de l'Union européenne, *Stratégie européenne de sécurité – Une Europe sûre dans un monde meilleur*, 2009, p. 43, en ligne à URL : <https://www.consilium.europa.eu/media/30810/qc7809568frc.pdf> consulté le 18 septembre 2023.

¹⁷⁸³ Parlement européen, Résolution du Parlement européen du 12 juillet 2007 sur l'accord avec les États-Unis d'Amérique concernant l'utilisation de données des dossiers des passagers aériens (PNR), 12 juillet 2007.

¹⁷⁸⁴ I. BECHROURI, « La 'guerre globale contre la terreur' : un discours contre-productif pour la lutte antiterroriste », *Les champs de mars*, n° 30, 2018, pp. 479-489.

¹⁷⁸⁵ 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.

¹⁷⁸⁶ M. BENLOLO-CARABOT, « Chronique Droit pénal de l'Union européenne – Protection des données personnelles, lutte contre le terrorisme : la CJUE confrontée à la surveillance de masse », *RTD eur.*, 2017, p. 887.

l'Europe récemment a certainement joué un rôle dans l'acceptation de cette tendance qui privilégie la sécurité collective aux droits individuels¹⁷⁸⁷.

La présente thèse a montré que les institutions européennes ont affiché des positions divergentes quant à la protection des données personnelles des passagers aériens. D'un côté, la nécessité de renforcer la sécurité publique est soulignée, tandis que de l'autre, l'importance de préserver les libertés fondamentales est mise en avant. Confrontées à la réalité des rapports de force dans les relations internationales, des institutions, tel le Conseil de l'Union européenne, ont manifesté une réticence à prioriser la protection de la vie privée et des données personnelles, affichant une position réaliste¹⁷⁸⁸. Le renoncement des principales institutions européennes à défendre vigoureusement les droits fondamentaux des passagers aériens a cependant été compensé par l'action de la CJUE, du Parlement et du Comité européen de la protection des données qui ont émergé en tant que garants des droits fondamentaux des passagers aériens¹⁷⁸⁹.

Précisément, cette étude met en lumière, dans une première partie, les obstacles traditionnels liés à la protection des données personnelles des passagers aériens. L'antagonisme entre les législations répressives américaines et européennes a mis en évidence l'obligation de transmission imposée par le droit américain et la contestation de celle-ci par les législations européennes. Les accords PNR ont permis l'échange de dossiers passagers sans une protection juridique effective, avec un risque d'empiètement sur le droit au respect de la vie privée et à la protection des données personnelles. De plus, nous avons examiné le rôle des institutions européennes dans la protection déséquilibrée des droits fondamentaux des passagers, en soulignant l'action contradictoire du Conseil de l'Union européenne et de la Commission par rapport au rôle de garant des droits fondamentaux joué par le Parlement européen, la CJUE, le Comité européen de la protection des données et le Contrôleur européen de la protection des données. Ces constats ont révélé les tensions inhérentes à la dialectique impératifs de sécurité publique et sauvegarde des droits individuels propre à la question complexe des dossiers passagers.

¹⁷⁸⁷ C. BERTRAM, « Notre guerre contre le terrorisme », in *Justifier la guerre*, Presses de Science Po, 2013, pp. 221-238

¹⁷⁸⁸ M. GALLET, « La France et l'Europe face à l'enjeu du Big Data, l'exemple de la collecte et du traitement des données médiatiques », *Géoéconomie*, 2014, pp. 7-23.

¹⁷⁸⁹ S. PEYROU, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », *EUROP* n° 7, juillet 2012, étude 8, en ligne à URL : <http://www.gdr-elsj.eu/2012/05/03/cooperation-policiere/diplomatie-ou-droits-fondamentaux-la-conclusion-de-laccord-pnr-entre-les-etats-unis-et-lunion/> consulté 15 janvier 2024.

Dans la seconde partie de l'étude, nous avons mis en exergue les nouvelles menaces pesant sur la protection juridique des dossiers passagers avec principalement deux aspects préoccupants. D'une part, l'affaiblissement de cette protection se manifeste dans le traitement des dossiers passagers aux frontières où des défis émergent quant à la conciliation entre impératifs sécuritaires et respect des droits fondamentaux. D'autre part, la déterritorialisation exerce une pression supplémentaire sur la protection juridique des dossiers passagers en soulevant des questions complexes liées à la territorialité des droits et à la responsabilité des acteurs impliqués.

De nos jours, la protection des données personnelles est, en effet, confrontée à de nouveaux défis en raison de la mondialisation et de l'évolution technologique peu régulée¹⁷⁹⁰. Le développement technologique a facilité la collecte et le partage massif de données personnelles, offrant aux entreprises et aux pouvoirs publics une utilisation étendue de ces informations. Dans un contexte où les individus partagent de plus en plus facilement des données personnelles à travers le monde, ces informations circulent librement en transformant les dynamiques économiques et sociales. Il a été mis en évidence que l'Union européenne n'est pas à l'abri de ce phénomène, car les données personnelles de ses citoyens sont transférées vers des pays tiers et des organisations internationales. Face à ces évolutions, il devient crucial de repenser les cadres réglementaires afin de garantir une protection adéquate des données personnelles dans ce paysage mondialisé et technologiquement avancé mais avec un risque de fragmentation. Les transferts de données personnelles des passagers aériens amplifient les conséquences du fichage aux frontières et suscitent des opinions divergentes. En raison de son étendue, cette collecte extensive de données personnelles peut constituer une surveillance généralisée et une intrusion dans la sphère privée des passagers¹⁷⁹¹.

Les données PNR deviennent également un outil de contrôle aux frontières¹⁷⁹². Or, le contrôle des visiteurs, caractérisé par la collecte étendue de données et la création de registres tels que les dossiers passagers, n'est pas sans implications et soulève le risque d'un affaiblissement de la protection juridique desdits dossiers dans la gestion des contrôles aux frontières. Ce système stocke des informations accessibles aux autorités frontalières, notamment à des fins d'enquête. Le système PNR offre aux services répressifs aux frontières la possibilité de prévenir et de détecter des infractions graves, notamment le terrorisme, en permettant

¹⁷⁹⁰ ¹⁷⁹⁰ L. OBADIA, « Technologies mondialisées, mondialisation technologique, Digital Globalization : quels liens entre les NTIC et la mondialisation ? », *Diogène*, vol. 271-272, n° 3-4, 2020, pp. 110-132.

¹⁷⁹¹ X. LATOUR, « Les fichiers PNR et les transports aériens internationaux », *Annuaire du droit de la sécurité et de la défense 2018*, Mare et Martin, 2018, pp. 247-258.

¹⁷⁹² J. LAGASSE, « 'Fichier' PNR : surveillance électronique de masse ou nouveau paradigme de la sécurité ? », *Les Notes du CREOGN*, 2016.

l'enquête et la poursuite des auteurs. L'analyse en temps réel des données PNR permet d'identifier des individus non-soupçonnés initialement mais dont les données indiquent une possible implication dans des infractions graves, nécessitant un examen approfondi des autorités compétentes. Aussi, ce système facilite la détection des personnes dont les déplacements sont suspects, tels les ressortissants européens soupçonnés de rejoindre des mouvements djihadistes. Cependant, il a également été souligné que la collecte massive et le profilage résultant de ces systèmes peuvent être perçus comme intrusifs, parce qu'ils impliquent la collecte et l'utilisation à long terme de toutes les informations liées aux passagers aériens. Il s'agit de menaces nouvelles qui pèsent sur les droits fondamentaux des passagers aériens.

Cette réflexion a souligné l'implication croissante des acteurs privés dans le contrôle des migrations¹⁷⁹³ qui est devenue une réalité incontournable pour les utilisateurs des transports aériens. Bien que la maîtrise des frontières reste une responsabilité fondamentale de l'État, il est désormais évident qu'il n'exerce plus seul cette mission mais avec la participation croissante de personnes privées, qu'il s'agisse de professionnels de la sécurité ou de transporteurs. Cette délégation à des acteurs privés, justifiée par l'incapacité des moyens étatiques à répondre pleinement aux besoins liés à la multiplication des mouvements migratoires, peut néanmoins contribuer à l'affaiblissement de la protection des dossiers passagers. Le recours accru à des acteurs privés, bien que pragmatique, soulève des questions fondamentales quant à la protection des données personnelles et la préservation des droits fondamentaux lors du contrôle des frontières.

L'opération la plus poussée qui se réalise aux frontières pour les passagers aériens est le profilage¹⁷⁹⁴ dont les conséquences sur les droits fondamentaux ont été étudiées dans cette thèse. L'objectif de l'opération est d'évaluer certains aspects personnels du passager aérien en vue de formuler un jugement ou d'en tirer des conclusions. Certaines de ces décisions sont totalement automatisées, prises par des algorithmes appliqués aux données personnelles, sans intervention humaine. Or, les décisions générées de manière automatique peuvent entraîner

¹⁷⁹³ Thales, « Le système électronique d'Entrée-Sortie en zone Schengen: la biométrie au service des frontières intelligentes », en ligne à URL : <https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/biometrie/systeme-entree-sortie> consulté le 15 janvier 2024.

¹⁷⁹⁴ A. MATTELART ET A. VITALIS, « Introduction. Les libertés au prix du contrôle », *Le profilage des populations. Du livret ouvrier au cybercontrôle*, sous la direction de Mattelart Armand, Vitalis André. La Découverte, 2014, pp. 5-11. Les auteurs notent que le profilage porte une menace pour les identités et les libertés individuelles, en déployant une puissance d'exploitation des données sans équivalent grâce à la déterritorialisation des traitements, à l'automatisation de la collecte, à la mise en œuvre d'algorithmes, ainsi qu'aux rapprochements et diffusions effectués. Le risque imminent, pour ces chercheurs, réside dans la convergence de l'automatisation avec l'autonomie de la technique.

des conséquences significatives sur les droits et les libertés d'un individu, notamment si elles restreignent l'accès à un service ou à un droit, tel le droit de se déplacer pour les passagers aériens, ou de réduire le passager à un aspect de son identité religieuse ou ethnique¹⁷⁹⁵. Le droit européen a ainsi imposé aux États membres de garantir qu'en cas de correspondance positive identifiée après un traitement automatisé des données des passagers aériens, une vérification individuelle soit réalisée par des moyens non automatisés. Cette démarche vise à déterminer si des mesures effectives doivent être prises conformément au droit en vigueur. Cela confirme la volonté du législateur de lutter contre l'empiètement du profilage¹⁷⁹⁶ sur le droit à la vie et à la protection des données à caractère personnel.

Dans cette seconde partie, nous avons également mis la lumière sur les acteurs du secteur aéroportuaire, tels que les transporteurs ou les professionnels de la sécurité¹⁷⁹⁷, qui jouent un rôle significatif¹⁷⁹⁸ en soulevant des préoccupations juridiques quant à la nécessité de réguler leur participation par les autorités publiques et de comprendre leur impact sur les droits fondamentaux des passagers aériens. En effet, outre l'affaiblissement de la protection juridique des dossiers passagers lié à l'ingérence des acteurs privés dans le traitement des données aux frontières, la privatisation des aéroports met en péril la protection de ces droits fondamentaux.

La privatisation des aéroports, notamment justifiée par la croissance continue du secteur aérien, pose des défis juridiques. Avec la multiplication des échanges et l'essor du tourisme de masse, le nombre d'usagers du transport aérien a considérablement augmenté. La surveillance des frontières offre un exemple où la privatisation des aéroports et la participation d'acteurs privés suscitent l'intérêt de grandes entreprises cherchant à répondre aux nouvelles menaces mondiales. En effet, cette recherche a montré toute la difficulté pour le législateur de s'assurer que les acteurs privés soient précautionneux quant au respect des standards de protection des données à caractère personnel alors que l'intérêt premier des entreprises est commercial. Dans ce contexte, les gouvernements européens doivent imposer des normes de protection très élevées pour les acteurs présents aux frontières, notamment dans les aéroports, afin de

¹⁷⁹⁵ T. HAMMARBERG, Commissaire aux droits de l'Homme du Conseil de l'Europe, « Le profilage racial et religieux n'a pas sa place dans la lutte anti-terroriste », 29 mai 2007, en ligne à URL : http://www.coe.int/t/commissioner/Viewpoints/070529_fr.asp consulté le 19 novembre 2023.

¹⁷⁹⁶ F. CASTAGNINO, « Critique des surveillances studies. Éléments pour une sociologie de la surveillance », *Déviance et Société*, vol. 42, n° 1, 2018, pp. 9-40.

¹⁷⁹⁷ H. PROTAR, *La sûreté aéroportuaire en France*, Université Panthéon-Assas-Paris II, 2016.

¹⁷⁹⁸ C. R. HAN, R. MCGAURAN, H. NELEN, « API and PNR data in use for border control authorities », *Security Journal*, 2016.

renforcer la sécurité intérieure et prévenir les attaques terroristes contre les aéroports européens.

Enfin, nous avons vu que le phénomène de déterritorialisation¹⁷⁹⁹, à savoir la rupture du lien entre le territoire et les individus ou la société, peut également mener à l'affaiblissement de la protection juridique des dossiers passagers. Il représente ainsi une autre menace nouvelle pour la protection juridique des dossiers passagers. La notion de rupture entre un territoire et des individus, ou un groupe, illustrent en l'espèce le processus de dissociation, de séparation ou de décontextualisation. S'agissant des relations de l'individu avec ses données figurant dans les dossiers passagers, la déterritorialisation est une menace : le passager voit ses données personnelles circuler dans le monde à chaque vol aérien qu'il effectue sans qu'il puisse forcément en avoir une pleine maîtrise.

Nous avons montré, au cours de notre réflexion, que les données à caractère personnel et les droits qui y sont associés se distendent¹⁸⁰⁰ en raison de l'absence d'un territoire commun¹⁸⁰¹ où la réalité juridique européenne, censée protéger le droit à la protection des données à caractère personnel, pourrait s'exercer concrètement et effectivement. Cette situation provoque une fragmentation des règles, rendant l'application uniforme des lois plus difficile. En effet, les dossiers passagers, qui suivent le passager aérien à travers ses voyages dans des centaines de destinations du monde, sont traités par des juridictions dont certaines ne reconnaissent pas le droit à la protection des données personnelles des passagers aériens.

Dans le dernier chapitre de la thèse, nous avons cependant apporté des nuances au processus de déterritorialisation¹⁸⁰² observé, caractérisé par des activités, des relations sociales et des influences dépassant les frontières traditionnelles des territoires nationaux pour devenir plus transnationales. Avec la multiplication des crises au cours de ces trente dernières années,

¹⁷⁹⁹ G. DELEUZE, F. GUATTARI, *L'Anti-Œdipe*, Minuit, 1972. Dans cet ouvrage, Deleuze et Guattari critiquent la psychanalyse freudienne, accusant cette dernière d'avoir reterritorialisé la libido sur le terrain du drame œdipien, après l'avoir libérée du psychisme grâce au concept de libido par le processus de déterritorialisation. Plus tard, en 1980, dans *Mille Plateaux*, les deux chercheurs français associent le concept de déterritorialisation au « corps-sans-organes » et introduisent la distinction entre « déterritorialisation relative » et « déterritorialisation absolue ».

¹⁸⁰⁰ F. POCHÉ, « Diagnostiquer le mécontentement », *Revue Projet*, 29 janvier 2020, en ligne à URL : <https://www.revue-projet.com/articles/2020-01-poche-diagnostiquer-le-mecontentement/10464> consulté le 12 juin 2023. L'auteur souligne l'émergence d'un présent saturé lié à la déterritorialisation constante permise par le numérique. La déterritorialisation numérique modifie le rapport des individus au monde, créant ainsi, selon le chercheur, un « malaise contemporain ». Cette analyse des changements induits par l'avènement de l'espace « numérique » adopte une perspective sociologique, critiquant la perte d'attention et la focalisation sur la « communauté d'élection ou d'origine, au détriment de la communauté de destin ».

¹⁸⁰¹ J-M PONTIER, « Territorialisation et déterritorialisation de l'action publique », *L'Actualité juridique*, Droit administratif, 1997.

¹⁸⁰² H. THERY, « Mondialisation, déterritorialisation, reterritorialisation », *Bulletin de l'Association de Géographes Français*, vol. 85-3, 2008, pp. 324-331.

phénomène aujourd'hui qualifié de polycrise¹⁸⁰³, on assiste à un retour de l'État en tant que réponse aux défis posés par la déterritorialisation. Ainsi, on assiste à une reterritorialisation qui se manifeste par l'action de certains acteurs politiques ou institutions qui cherchent à renforcer leur contrôle et leur influence dans des territoires spécifiques, en réponse aux défis économiques, politiques ou sociaux liés à la mondialisation et à la déterritorialisation.

Dans le domaine de la protection des données à caractère personnel des passagers aériens, surtout depuis la crise sanitaire du Covid-19, on a observé un processus par lequel les acteurs gouvernementaux tentent de renforcer leur pouvoir et leur contrôle dans la gestion des flux de passagers aériens pour faire face aux défis posés par la pandémie. Cela s'est concrétisé notamment par des investissements dans le contrôle aux frontières nationales et dans les technologies visant à une meilleure maîtrise de l'espace géographique, y compris les dans les plateformes aéroportuaires. Cette crise sanitaire a aussi offert un prétexte à certains gouvernements pour justifier un « pillage massif » des données de leurs citoyens au nom de la protection de la collectivité et de la lutte contre la pandémie, notamment en Chine. Dans ces cas, il n'y a eu que très peu de considérations pour la protection des données à caractère personnel. On assiste donc à un retour de l'État dans un domaine dans lequel il tendait auparavant à laisser de plus en plus de place aux opérateurs privés.

Ces dynamiques mentionnées dans la seconde partie de notre étude convergent pour créer un paysage complexe et en évolution constante, exigeant une réflexion continue sur les moyens de garantir une protection juridique robuste des dossiers passagers tout en relevant les défis posés par les évolutions rapides de la gestion des données et des impératifs sécuritaires. Face à ces enjeux, il devient impérieux de développer des cadres juridiques visant un équilibre entre la nécessité de préserver la sécurité collective et le respect inébranlable des droits fondamentaux des individus, en particulier s'agissant de la question sensible des données passagers.

¹⁸⁰³ J-M. POTTIER, « Polycrise », Sciences humaines, *Actualité de la recherche*, mensuel n° 358, mai 2023.

BIBLIOGRAPHIE

1. OUVRAGES

A. Ouvrages de droit

Agence des droits fondamentaux de l'Union européenne, *Manuel de droit européen en matière de protection des données*, éd. 2018.

K. BANNELIER, T. CHRISTAKIS, O. CORTEN et B. DELCOURT, *Le droit international face au terrorisme*, Paris, Pedone, 2012, p. 116.

C. BECCARIA, *Des délits et des peines*, 1764.

L. BERNARDEAU, *Les amendes en droit de la concurrence*, Bruxelles, Larcier, 2013.

G. BOISMENU, I. PETIT, *L'Europe qui se fait : Regards croisés sur un parcours inachevé*, Presses de l'Université de Montréal, 2008 ; en ligne sur : <http://books.openedition.org/pum/15196> consulté le 2 novembre 2023.

I. BOUHADANA, W. GILLES (dir.), *Cybercriminalité, cybermenaces & cyberfraudes*, Les éditions IMOD-V, 2012.

A. BRADFORD, "The Brussels Effect. How the European Union rules the World", Oxford, Oxford University Press, 2020.

J. CARBONNIER, *Flexible droit. Pour une sociologie du droit sans rigueur*, LGDJ, coll. « Anthologie du droit », 2013.

B. CASSEN, H. MICHEL, L. WEBER, *Le Parlement européen, pour faire quoi ?*, Brignais, Éditions du Croquant, 2014.

J. CEDRAS, *Droit pénal américain*, PUF, coll. « Que sais-je ? », 1997.

V. CORREIA, *L'Union européenne et le droit international de l'aviation civile*, Bruxelles, Bruylant, 2014.

O. COSTA, *Le Parlement européen, assemblée délibérante*, Bruxelles, Éditions de l'Université de Bruxelles, 2001.

A. DELBLOND, *Droit administratif*, Larcier, collection Manuels Larcier, 2009.

J. S. GRANICK, *American spies: modern surveillance, why you should care, and what to do about it*, Cambridge University Press, 2017.

S. HENRY, *L'Union européenne, une construction sui generis*, Ellipses, Droit de l'Union européenne, coll. « Tout-en-un droit », 2020.

R. A. KAGAN, *Adversarial Legalism. The American Way of Law*, Harvard University Press, 2003.

- P. KLÖTGEN, *La frontière et le droit, esquisse d'une problématique*, Scientia Juris, 2011.
- R. MILLER, *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, Cambridge University Press, 2017.
- T. RAMBAUD, *Introduction au droit comparé. Les grandes traditions juridiques dans le monde*, Paris, PUF, 2014.
- C. ROUSSEAU, *Droit international public*, Paris, Sirey, 1977.
- F. TERRE, *Introduction générale au droit*, Paris, Dalloz, 8^e éd., 2009.
- A. VAUCHEZ, *L'Union par le droit. L'invention d'un programme institutionnel pour l'Europe*, Paris, Presses de Science Po, 2013.
- J-C. ZARKA, *L'essentiel des institutions de l'Union européenne*, Lextenso, 2020.

B. Ouvrages sur les libertés publiques

- T. BINGHAM, *The rule of law*, Allen Lane, 2020.
- D. COLE, J. DEMPSEY, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*, New York, New Press, 2002.
- E. HINTON, *From The War On Poverty To The War On Crime: The Making Of Mass Incarceration in America*, Cambridge, Harvard University Press, 2016.
- R. KEMPF, *Ennemis d'États. Les lois scélérates des anarchistes aux terroristes*, La Fabrique éditions, 2019.
- A. PETROPOULOU, *Liberté et sécurité : les mesures antiterroristes et la Cour européenne des droits de l'Homme*, Paris, Éditions A. Pedone, 2014.
- S. SASSEN, *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton University Press, 2006.
- S. M. SMYTH, *Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control*, New York, Routledge, 2019.

C. Autres ouvrages

- B. BADIE, *La fin des territoires*, Paris, Fayard, 1995.
- R. BOYER, *Les capitalismes à l'épreuve de la pandémie*, Paris, La Découverte, 2021.
- R. CARTER, *La sûreté des transports. Les transports face aux risques et menaces terroristes*, Paris, PUF, 2008.
- A. CRAWFORD (ed.), *Crime and insecurity: the governance and safety in Europe*, Cullompton, Willan, 2002.

R. DEBRAY, *Civilisation, Comment nous sommes devenus américains*, Gallimard, « coll. Blanche », 2017.

G. DELEUZE, F.GUATTARI, *L'Anti-Œdipe*, Minuit, 1972.

G. DELEUZE, F.GUATTARI, *Mille plateaux*, Minuit, 1980.

A. DERSHOWITZ, *Why Terrorism Works: Understanding the Threat, Responding to the Challenge*, New Haven, Yale University Press, 2002.

E. DURKHEIM, *La division du travail social*, 1893.

J. FERNANDEZ, J-V. HOLEINDRE, *Nations désunies ? La crise du multilatéralisme dans les relations internationales*, CNRS, Biblis Inédit, 2022.

D. P. FIDLER, *The Snowden Reader*, Indiana University Press, 2015.

P. FONTAINE, *L'Union européenne. Histoire, institutions, politiques*, Points, 3 mai 2012.

J. GARRIGUES, *La defensa de la competencia mercantil*, Madrid, 1964.

A. GORDON, *Naked airport: a cultural history of the world's most revolutionary structure*, University of Chicago Press, 1^{er} juin 2008.

V. HEYDON, S. WOODCOCK, *The rise of bilateralism: comparing American, European and Asian approaches to preferential trade agreements*, UN University Press, 2009.

T. HOBBS, *Léviathan*, 1651.

V. HUGO, *Océan Prose*, in *Œuvres complètes*, 1854, R. Laffont, 1995.

S. LAURENT, *Politiques du renseignement*, Pessac, Presses Universitaires de Bordeaux, 2009.

K. LE BOURHIS, *Les transporteurs et le contrôle des flux migratoires*, Paris, L'Harmattan, 2001.

M. LEFEBVRE, *La politique étrangère européenne*, Paris, PUF, 2021.

J. MONNET, *Mémoires*, Fayard, 1976.

M. OULD SLAHI, *Les carnets de Guantanamo*, Michel Lafon, 2015.

B. PASCAL, *Œuvres complètes*, II, Paris, Gallimard, Bibl. La Pléiade, « Pensées », 2000.

O. ROY, *Le djihad et la mort*, Éditions Seuil, 2016.

J.-J. ROUSSEAU, *Discours sur l'origine et les fondements de l'inégalité parmi les hommes – Discours sur les sciences et les arts*, Partie II, Paris, Flammarion, 1995.

E. W. SAÏD, *Orientalism*, Pantheon Books, 1978.

G. SALINES, *L'Indicible de A à Z*, Paris, Seuil, 2016.

D. SOGGE, *La crise du multilatéralisme. Enjeux et défis du développement international : Acteurs et champs d'action. Édition nouvelle et actualisée*, Les Presses de l'Université d'Ottawa, 2019.

D. THOMSON, *Les Revenants, Ils étaient partis faire le jihad, ils sont de retour en France*, Éditions Seuil, 2016.

M. TORGA, *L'universel, c'est le local moins les murs*, William Blake, 2010.

A. TOURAINÉ, *Un nouveau paradigme pour comprendre le monde d'aujourd'hui*, Fayard, 2005.

D. WILLS, *The First War on Terrorism: Counter Terrorism during the Reagan Administration*, Lanham, Rowman and Littlefield, 2003.

2. THÈSES, MÉMOIRES

A. Thèses

J. HARIVEL, *Libertés publiques, libertés individuelles, risques et enjeux de la société numérique*, Droit, Université Panthéon-Sorbonne - Paris 1, 2018.

Z. HATTAB, *Droits et libertés fondamentaux en droit musulman : le paradoxe de l'universalité*, Droit, Université d'Avignon, 2018.

W. MAXWELL, *Le contrôle humain des systèmes algorithmiques. Un regard critique sur l'exigence d'un humain dans la boucle*, Droit, Université Panthéon-Sorbonne - Paris 1, 2022.

B. Mémoires

M. E. LEVEILLE, *Le profilage ethno-racial aux États-Unis : analyse juridique et historique avant et après le 11 septembre 2001*, mémoire de l'Institut d'études politiques de Paris, février 2003.

H. PROTAR, *La sûreté aéroportuaire en France*, Mémoire de Master, Université Panthéon-Assas-Paris 2, 2016.

M. WOZNY, *Exploitation des données personnelles : raison commerciale, raison d'état et opportunités*, Mémoire, Université de Lyon, août 2017.

3. ARTICLES DE REVUES SCIENTIFIQUES

A. ADAM, « L'échange de données à caractère personnel entre l'Union européenne et les États-Unis », *Revue de droit européen*, Dalloz, 2006.

P. AIGRAIN, « Porte ouverte à la surveillance et à la suspicion généralisées », *Dalloz*, Pénal, 24 mars 2015 ; en ligne sur : <https://www.dalloz-actualite.fr/chronique/porte-ouverte-surveillance-et-suspicion-generalisees>

- S. AKRAM, K. JOHNSON, « Race, civil rights, and immigration law: after September 11, 2001: the targeting of Arabs and Muslims », *New York University Annual Survey of American Law*, n° 58, 2002, pp. 295-355.
- V. ALBERTO, D. BOGATZ, Computer Assisted Passenger Prescreening System (“CAPPS II”), National Security V. Civil Liberties, 19 mai 2004.
- A. ALIBEIGI, A. MUNIR, M. KARIM, “Right to Privacy, A Complicated Concept to Review”, *SSRN Electronic Journal*, 2019.
- J. ALIX, O. CAHN, « Mutations de l’antiterrorisme et émergence d’un droit répressif de la sécurité nationale », *Revue de science criminelle et de droit pénal comparé*, 2017, pp. 845-868.
- M. A. AL-MIDANI, « La ligue des États arabes et les droits de l’Homme », *Scienza & Politica*, juin 2002 ; en ligne sur : <https://doi.org/10.6092/issn.1825-9618/2892>
- B. E. ALTSCHULER, Review of American Surveillance: Intelligence, Privacy, and the Fourth Amendment, by A. GREGORY, *Political Science Quarterly*, 132(4), 2017, pp. 755–757 ; en ligne sur : <http://www.jstor.org/stable/45175877>
- D. M. AMANN, « Le dispositif américain de lutte contre le terrorisme », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2000.
- E. E. ANDERSON, J. CHOUBINEH, « Enterprise information security strategies », *Computers & Security*, Vol. 27, p. 23, 2008.
- C. ANZIEU-PREMMEREUR, « Après le 11 septembre 2001 à New York », *Revue française de psychanalyse*, 2003, pp. 865-876.
- L. ARCHAMBAULT, B. TIGAUD, « La directive PNR et son articulation avec le RGPD : l’instauration d’un fichier de données des passagers aériens, outil efficace de la lutte contre le terrorisme et respectueux des données personnelles », *Gazette du Palais*, LGDJ, n° 6, 12 février 2019.
- S. ASHAR, « Immigration enforcement and subordination: the consequences of racial profiling after September 11 », *Connecticut Law Review*, n° 34, 2002, pp. 1185-1199.
- S. AUDOIN-ROUZEAU, « L’après-13 Novembre, Naissance et mort d’une ‘culture de guerre’ ? », *Vingtième siècle. Revue d’histoire*, n° 134, 2017, p. 11.
- E. AUTIER, « La CJUE déclare incompatible l’accord des données PNR signé avec le Canada », *Dalloz*, 28 juillet 2017.
- O. CACHARD, « Le transport international aérien de passagers », *Académie de droit international de La Haye*, 2015.

E. BARBRY, « Le droit à la protection des données personnelles n'est pas un droit absolu face à la liberté d'information », *Le Monde du Droit*, 9 juillet 2021.

A. BARILARI, « La fraude fiscale : les mots et les chiffres », *Gestion et finances publiques*, 2018/3, pp. 50-57 ; en ligne sur : <https://www.cairn.info/revue-gestion-et-finances-publiques-2018-3-page-50.htm>

A. BARNETT, "CAPPS II: The Foundation of Aviation Security?", *Risk Analysis*, Volume 24, Issue 4, 2004, pp. 909-916.

D. BATORSKI, Z. SMOREDA, « La diffusion des technologies d'information et de communication, Une enquête longitudinale en Pologne », *Réseaux*, 2007, pp. 193-221.

V. BAZZOCCHI, « L'accord entre l'Union européenne et les États-Unis sur les données PNR », *European rights*, 2007 ; en ligne sur : http://www.europeanrights.eu/public/commenti/Commento_Valentina_Bazzocchi_Accordo_PNR.pdf

I. BECHROURI, « La 'guerre globale contre la terreur' : un discours contre-productif pour la lutte antiterroriste », *Les champs de mars*, n° 30, 2018, pp. 479-489.

R. BELLANOVA, D. DUEZ, « Le citoyen face aux nouvelles pratiques sécuritaires de l'Union européenne : enjeux démocratiques d'une sécurité par les fichiers », *Espace populations sociétés*, 2012/3, pp. 49-62 ; en ligne sur : <http://journals.openedition.org/eps/5104>

V.-L. BENABOU, « L'extension du domaine de la donnée », *Légipresse*, n° 359, avril 2018.

B. BENHAMOU, « L'internet des objets. Défis technologiques, économiques et politiques », *Esprit*, n° 3-4, 2009, pp. 137-150.

M. BENLOLO-CARABOT, « Chronique Droit pénal de l'Union européenne – Protection des données personnelles, lutte contre le terrorisme : la CJUE confrontée à la surveillance de masse », *La Revue trimestrielle de droit européen*, Dalloz, 2017.

J-C. BEAUJOUR, « La nouvelle donne internationale et les opportunités de coopération stratégique UE/Chine », *Revue Défense Nationale*, Revue n° 838 Mars 2021, p. 83-89.

M. BERGADAÀ, « Le temps économique et le temps psychologique du voyageur dans un aéroport international », *La revue des sciences gestion*, 2009/2, n° 236, pp. 12-23.

N. BERMAN, "Privileging Combat? Contemporary Conflict and the Legal Construction of Law," *Columbia Journal of Transnational Law*, vol. 43, n° 1 (2004), pp. 32-33.

E. BERNARD, « Commission européenne », *Dalloz*, décembre 2019.

M. BERNELIN, S. DESMOULIN, T. LEFEVRE, « Données massives, big data et santé publique », *ADSP*, n° 112, 13 septembre 2020.

- P. BERTHELET, « Tous les chemins mènent... à Luxembourg. Analyse institutionnelle de l'accord PNR UE-Canada », *RDLF*, Droit de l'Union européenne, Chronique n° 20, 2018 ; en ligne sur : <https://revuedlf.com/droit-ue/tous-les-chemins-menent-a-luxembourg-analyse-institutionnelle-de-laccord-pnr-ue-canada/>
- P. BERTHELET, Y. EL BOUSTANI, L. FÉRIEL, L. ROBERT, N. PRADEL..., « Le volet externe de l'espace de liberté, de sécurité et de justice : instruments et réalisations », *Revue trimestrielle de droit européen*, Dalloz, 2014.
- A. BERY, L. DELPRAT, « Les nouveaux délais de conservation des dossiers médicaux », *Art*, 2008.
- A. BIAVA, « L'Union européenne, acteur global ? Potentialités et limites de la PESC et de la PESD », *Europa*, Institut européen de l'Université de Genève, 2005.
- K. BIEDENKOPF, O. COSTA, M. GÓRA, « Introduction: shades of contestation and politicization of CFSP », *European Security*, 2021, pp. 325-343.
- C. BILLET, « L'échange et la protection de données avec les États tiers : un nouveau volet prioritaire de l'action extérieure de l'Union ? », *RTDEur.*, Dalloz, n° 3, 2000.
- C. BILLET, « L'échange et la protection de données avec les États tiers : un nouveau volet prioritaire de l'action extérieure de l'Union ? », *Revue trimestrielle de droit européen*, 2020.
- P. BIPLAN, « Les compagnies aériennes entre la nation et la mondialisation », *Hérodote*, 2004, pp. 56-70.
- V. BONED, B. CRESPIN, O. KERVELLA et autres, « La crise sanitaire : accélérateur de changement dans le tourisme », *Juris Tourisme*, Activités touristiques, Dalloz, n° 240, 2021, p. 39.
- R. BOUCQ, « Schrems II : répercussion française », *Administratif IP/IT et Communication*, Dalloz, 21 octobre 2020 ; en ligne sur : <https://www.dalloz-actualite.fr/node/schrems-ii-repercussion-francaise>
- M. BOUCTON, S. PARIER, « La sûreté aéroportuaire : oui, mais à quel prix ? », *Air & Cosmos*, n° 2564, octobre 2017.
- M. BOURGEOIS, L. THIBIERGE, « Droit de la donnée : plaider pour un régime général », Données personnelles, *La Semaine Juridique Entreprise et Affaires*, n° 20, 14 mai 2020.
- C. BRÉCHON-MOULÈNES, « Marchés publics », *Répertoire de droit international*, Dalloz, mars 2009.
- R. BRETT, « La directive "PNR" du 27 avril 2016, nouvelle étape de la politique européenne de lutte contre la criminalité », *Protection des données personnelles*, Europe, étude 1, 2017.

- D. BROUSSOLLE, « Société de transports », *Répertoire des sociétés*, Dalloz, décembre 2010.
- J. BRUTON, « La relation euro-américain en transition », *Politique américaine*, L'Harmattan, 2006/3, pp. 15-24.
- C. BUNZEL, "Jihadism on its own terms", *Hoover Institution Press*, 2017.
- F. CABASINO, « Les attentats du 11 septembre. Émotion et raison dans la presse en France et en Italie », *Mots. Les langages du politique*, 2004, pp. 21-33.
- P. CADIO, F. NGUYEN, « RGPD/PIPL : superposition et empiètement des réglementations sur la protection des données personnelles des citoyens d'Europe et de Chine », *LpaLaw*, Option Finance n° 1662, 4 juillet 2022, en ligne sur : <https://www.lpalaw.com/wp-content/uploads/2022/07/2022.07-Option-Finance--PIPL-RGPD.pdf>
- C. CALOTHY, « Face au terrorisme, progrès et limites d'une coopération internationale tous azimuts », *Pouvoirs*, La lutte contre le terrorisme, Le Seuil, 2016, pp. 125-137.
- E. CARPANELLI, N. LAZZERINI, "PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU", *Air and Space Law*, vol. 42, Issue 4/5, 2017, pp. 377-402.
- S. CARRERA, E. GUILD, "Does the Stockholm Programme matter?, The struggles over ownership of AFSJ", Multiannual programming, *Liberty and security in Europe*, n° 51, 2012 ; en ligne sur : [http://aei.pitt.edu/38964/1/No_51_Carrera_and_Guild_on_Stockholm_Programme\[1\].pdf](http://aei.pitt.edu/38964/1/No_51_Carrera_and_Guild_on_Stockholm_Programme[1].pdf)
- D. CARREAU, P. JUILLARD, « Négociations commerciales internationales », *Répertoire de droit international*, Dalloz, août 2017.
- B. CASSAR, « Données – gouvernance des données », *Répertoire IP/IT et Communication*, Dalloz, mars 2022.
- C. CASTETS-RENARD, « La protection des données personnelles dans les relations internes à l'Union européenne, la protection des données personnelles en matière civile et commerciale », *Répertoire de droit européen*, Dalloz, novembre 2022.
- A. CEYHAN, « Les technologies européennes de contrôle de l'immigration, vers une gestion électronique des 'personnes à risque' », *Réseaux*, 2010, pp. 131-150.
- F. CHALTIEL, « Le Traité de Lisbonne : la réforme du système contentieux européen - L'État de droit européen renforcé », *Petites affiches*, Lextenso, 2008.
- F. CHALTIEL, « L'équilibre entre sécurité et liberté devant le juge constitutionnel », *Actu-juridique*, Droit constitutionnel, 11 juillet 2019 ; en ligne sur : <https://www.actu-juridique.fr/constitutionnel/lequilibre-entre-securite-et-liberte-devant-le-juge-constitutionnel/>

- J. CHICHIZOLA, « Vingt ans après, les fantômes d'al-Qaida hantent toujours l'antiterrorisme français », *Le Monde*, 25 mai 2023 ; en ligne sur : <https://www.lefigaro.fr/actualite-france/vingt-ans-apres-les-fantomes-d-al-qaida-hantent-toujours-l-antiterrorisme-francais-20230522>
- S. H. CLEVELAND, P. B. STEPHAN, « Introduction: The Roles of the Restatements in U.S. Foreign Relations Law », in *The Restatement and Beyond: The Past, Present, and Future of U.S. Foreign Relations Law*, New York, *Oxford Academic*, 22 octobre 2020.
- M.-A. COHENDET, « Le droit répressif, quelles valeurs, quelles frontières ? », *Revue juridique de l'environnement*, Lavoisier, 2014.
- F. COLLART DUTILLEUL, « L'harmonisation internationale du droit privé », *Revue générale de droit*, Droit comparé, vol. 24, n° 2, 2 juin 1993 ; en ligne sur : <https://id.erudit.org/iderudit/1056952ar>
- V. CORREIA, « À propos de l'avis 1/15 relatif au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens », *Communication – Commerce électronique*, n° 6, LexisNexis, juin 2018.
- V. CORREIA, « Fasc. 978 : Données des passagers aériens », *JurisClasseur Communication*, LexisNexis, 15 novembre 2019.
- A. DAUCHY, “Dreaming biometrics in Niger: The security techniques of migration control in West Africa”, *Security Dialogue*, 2023.
- A. DEBET, « Profilage – APB enfin remis en cause ! », *Communication Commerce électronique*, Dalloz, 2017.
- E. DEBIES, « Renforcement des droits des individus sur leurs données personnelles : quelles conséquences sur l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) ? », *Regards*, 2019, pp. 149-155.
- M. DE FALLOIS, « Les traitements de données de santé à des fins de recherche liés à la COVID-19 : quelle régulation par la CNIL ? », *Journal du droit de la santé et de l'assurance – Maladie*, 2021, pp. 26-32.
- P. DE HERT, V. PAPAKONSTANTINO, “The PNR Agreement and Transatlantic Anti-terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic”, *AARN: Topics of Concern in Applied Anthropology (Topic)*, Law, 1^{er} juin 2009 ; en ligne sur : <https://www.semanticscholar.org/paper/The-PNR-Agreement-and-Transatlantic-Anti-terrorism-Hert-Papakonstantinou/c37bfdfd20026061e97bd8ed5b1e48dfca1d03c4>
- X. DELPECH, « Un rapport critique sur les privatisations d'aéroports », *Juris tourisme*, Transport aérien, Dalloz, n° 214, JT 2018.

- X. DELPECH, « La directive PNR confrontée au respect des droits fondamentaux », *Affaires, IP/IT et Communication*, Droits fondamentaux, Dalloz, 19 septembre 2022 ; en ligne sur : <https://www.dalloz-actualite.fr/flash/directive-pnr-confrontee-au-respect-des-droits-fondamentaux>
- P. DELVOLVÉ, « La privatisation du service de l'État », *Pouvoirs*, vol. 117, n° 2, 2006, pp. 107-120.
- G. DE MÉNIL, « L'importance historique du plan Marshall », *Commentaire*, 2022/2, n° 178, 2022.
- V. DEMERTZIS, « Élire le Parlement européen », *Courrier hebdomadaire du CRISP*, 2014, pp. 5-100.
- M. DEN BOER, « 9/11 and the europeanisation of anti-terrorism policy: a critical assessment », *Groupeement d'études et de recherches « Notre Europe »*, Paris, 2003
- E. DERIEUX, « Vie privée et données personnelles – Droit à la protection et "droit à l'oubli" face à la liberté d'expression », *Les nouveaux cahiers du Conseil constitutionnel*, 2015, pp. 21-31 ; en ligne sur : <https://www.cairn.info/revue-les-nouveaux-cahiers-du-conseil-constitutionnel-2015-3-page-21.htm>
- O. DE SCHUTTER, « Les droits fondamentaux dans l'Union européenne », *Journal de droit européen*, 2012, p. 114.
- A. DIEHL, « Le GDPR, cette nouvelle loi qui va tout changer », *Abondance, lettre Recherche et Référencement*, avril et mai 2017 ; en ligne sur : <http://recherche-referencement.abondance.com/2017/04/le-gdpr-cette-nouvelle-loi-qui-va-tout.html>
- S. DIMITROULIAS, « L'humanisme juridique européen à l'épreuve du terrorisme : le crépuscule de la clémence ? », *L'Homme & la Société*, 2006, pp. 111-132.
- C. DOCKSEY, « Opinion 1/15: Privacy and security, finding the balance », *Maastricht Journal of European and Comparative Law*, vol. 24, n° 6, 2017, pp. 768-773.
- K. DOUPLITZKY, « Le commerce de moi, modèle économique du profilage », *Traçabilité et réseaux, Hermès La Revue*, 2009, pp. 113-117.
- J. DRYDEN, « Un monde sans frontières : concrétiser le potentiel du commerce électronique mondiale », *L'Observateur de l'OCDE*, 1999.
- P. DU BOIS, « L'Union européenne et les droits de l'Homme », *Relations internationales*, 2007, pp. 33-39.
- E. DUBOUT, « Principes, droits et devoirs dans la Charte des droits fondamentaux de l'Union européenne », *RTDE*, Dalloz, 2014.

F. DUBUISSON, « La définition du ‘terrorisme’ : débats, enjeux et fonctions dans le discours juridique », *Confluences méditerranée*, 2007, pp. 29-45.

D. DUEZ, « De la définition à la labellisation : le terrorisme comme construction sociale », in Digwatch, « The G20 Osaka Track raises controversy », 1^{er} juillet 2019 ; en ligne sur : <https://dig.watch/updates/g20-osaka-track-raises-controversy>

O. DUFOUR, M.-A. FRISON-ROCHE, « La nouvelle loi de protection des données en Chine est un ‘anti-RGPD’ », *Actu-juridique*, 2 septembre 2021 ; en ligne sur : <https://www.actu-juridique.fr/ntic-medias-presse/la-nouvelle-loi-de-protection-des-donnees-en-chine-est-un-anti-rgpd/>

P. DUPONT, « Les données des dossiers passagers (PNR) dans le transport aérien », *Revue française de droit aérien et spatial*, vol. 278, n° 2, 2016.

P. DUPONT, « La souveraineté aérienne et les frontières de la troisième dimension », *Revue défense nationale*, 2023, pp. 157-161.

J. DUTHEIL DE LA ROCHÈRE, « Droit au juge, accès à la justice européenne », *Pouvoirs*, 2001, pp. 123-141.

R. DWORKIN, R. ROBERT, M.-O. PADIS, « George W. Bush, une menace pour le patriotisme américain », *Esprit*, 2002, pp. 6-23 ; en ligne sur : <http://www.jstor.org/stable/24279185>

R. B. EDELMAN, B. RICHARD, H. KENT BAKER, “The impact of implementing the airline deregulation act on stock returns”, *Journal of Economics and Finance*, 1996, pp. 79-99.

EGMONT INSTITUTE, « Pacte de la Ligue des États Arabes », *Jstor*, 22 mars 1945, en ligne sur : <https://www.jstor.org/stable/44827318>

D. EMMANUEL, P. FLORA, « Cybersécurité et objets connectés », *Dalloz IP/IT*, 2016.

C. EMANUELLI, Faut-il parler d’une “guerre” contre le terrorisme? *Canadian Yearbook of international Law/Annuaire canadien de droit international*, 2009.

J. EYNARD, « D'une ingérence généralisée à une autre : deux poids, deux mesures ? », *Revue trimestrielle des droits de l'Homme*, 2018, pp. 761-783.

E. FAHEY, E. GUILD, E. KUSKONMAZ, “The novelty of EU passenger name records (PNR) in EU trade agreements: on shifting uses of data governance in light of the EU-UK trade and cooperation agreement PNR provisions”, *European papers*, 2023 ; en ligne sur URL: https://www.europeanpapers.eu/en/system/files/pdf_version/EP_eJ_2023_1_4_Articles_EFah_ey_EGuild_EKuskonmaz_00651.pdf

- L. FARET, « Enjeux migratoires et nouvelle géopolitique à l'interface Amérique latine-États-Unis », *Hérodote*, 2018, pp. 48-105.
- C. FÉRAL-SCHUHL, *Données en matière pénale*, Dalloz, Praxis Cyberdroit, Chapitre 134, 2021.
- C. FÉRAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », *Praxis CyberDroit*, Dalloz, 2020-2021.
- C. FÉRAL-SCHUHL, « Des droits de la personne renforcés », Les données personnelles, *Praxis Cyberdroit*, Dalloz, 2020-2021.
- C. FÉRAL-SCHUHL, « Transfert des données à caractère personnel hors de l'Union européenne », *Praxis CyberDroit*, Dalloz, 2020-2021.
- J. FERGUSSON, « Canada aux marges », *Outre-terre*, 2006, pp. 362-368 ; en ligne sur : <https://www.cairn.info/revue-outre-terre2-2016-4-page-362.htm>
- G. FERRAGU, « L'invention du mythe terroriste : la Russie et ses Démons », *Histoire du Terrorisme*, 2014, pp. 61-95.
- L. FINNEGAN ABDOLIAN, H. TAKOOSHIAN, "The USA Patriot Act: Civil Liberties, the Media, and Public Opinion", *30 Fordham Urb. L.J.* 1429, 2003 ; en ligne sur : <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2097&context=ulj>
- J.-P. FOEGLE, « Protection des données personnelles : un droit fondamental menacé », *Plein droit*, 2016, pp. 41-48 ; en ligne sur : <https://www.cairn.info/revue-plein-droit-2016-3-page-41.htm>
- J.-P. FOEGLE, « Chronique du droit "Post-Snowden" : la CJUE et la CEDH sonnent le glas de la surveillance de masse », *La Revue des droits de l'Homme*, Actualités Droits-Libertés, 30 mars 2016 ; en ligne sur : <https://journals.openedition.org/revdh/2074>
- C. FORGET, « La protection des données dans le secteur de la police et de la justice », *Larcier*, Le règlement général sur la protection des données, Dalloz, 2018.
- E. FRIEDEL-SOUCHU, « Extraterritorialité du droit de la concurrence aux États-Unis et dans la Communauté européenne », *Revue critique de droit international privé*, Dalloz, 1995.
- G. FROMM, « Psychanalyse et trauma : retour sur le 11 septembre », *Diogène*, n° 203, 2003, pp. 3-19.
- C. GAGLIO, S. GUILLOU, « L'Europe numérique, entre singularités, faiblesses et promesses », *Revue de l'OFCE*, 2018, pp. 11-36.
- P. GAIA, « La Charte des droits fondamentaux de l'Union européenne », *Revue française de droit constitutionnel*, n° 58, 2004, pp. 227-246.

M. GALLET, « La France et l'Europe face à l'enjeu du Big Data, l'exemple de la collecte et du traitement des données médiatiques », *Géoéconomie*, 2014, pp. 7-23.

A. GALY, « La gestion des frontières par le traitement différencié des voyageurs. Réflexion croisée sur la France et les États-Unis », *Critique internationale*, vol. 93, n° 4, 2021, pp. 137-155.

A. GARAPON, « Les dispositifs antiterroristes de la France et des États-Unis », *Esprit*, n° 327, août-septembre 2006, pp. 125-149.

V. GAUTRON, D. MONNIAUX, « De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme », *Archives de politique criminelle*, 2016, pp. 123-135.

R. GAY, K. GUILLAS-CAVAN, « La gestion sanitaire de l'épidémie de Covid-19 par les États : recettes communes et logiques nationales », *Chronique international de l'IRES*, 2020/3, n° 171, 2020 ; en ligne sur : <https://www.cairn.info/revue-chronique-internationale-de-l-ires-2020-3-page-3.htm&wt.src=pdf>

M. P. GIBNEY, "The Extraterritorial Application of U.S. Law: The Perversion of Democratic Governance, the Reversal of Institutional Roles, and the Imperative of Establishing Normative Principles", *Boston College International & Comparative Law Review*, 1996 ; en ligne sur : <https://lira.bc.edu/files/pdf?fileid=63ad7b27-4fa1-4027-836c-3c67f6d8e464>

J.-E. GICQUEL, « Le droit de l'antiterrorisme - Un droit aux confins du droit administratif et du droit pénal », *La Semaine juridique Édition générale*, n° 40, 2 octobre 2017.

P. GILLIAUX, « La force obligatoire de la Charte des droits fondamentaux de l'Union européenne », *Revue trimestrielle des droits de l'Homme*, 2022, pp. 69-102.

A. D. GIVENS, N. E. BUSCH, D. A. BERSIN, « Going Global: The International Dimensions of U.S. Homeland Security Policy », *Journal of Strategic Security*, 11, n° 3, 2018, pp. 1-34 ; en ligne sur : https://digitalcommons.usf.edu/jss/vol11/iss3/2/?utm_source=digitalcommons.usf.edu%2Fjss%2Fvol11%2Fiss3%2F2&utm_medium=PDF&utm_campaign=PDFCoverPages

J. GOLDSMITH, C. SUNSTEIN, « Military tribunals and legal culture : what a difference sixty years make », *Public Law and Legal Theory Working Paper*, n° 27, 2002, p. 14 ; en ligne sur : https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=12361&context=journal_articles

J.-B. GOSSÉ, A. SCHNEIDER, R. VICQUÉRY, « Les leçons du plan Marshall pour le plan de relance européen », *Bloc-notes Eco*, Banque de France, 29 octobre 2021.

P. GOSSELIN, « Les libertés individuelles et collectives à l'heure du numérique et de l'état d'urgence sanitaire », Gouverner à l'ère numérique, *L'ENA hors les murs*, 2020, pp. 10-12.

M.-C. GRANGER, « Existe-t-il un droit fondamental à la sécurité ? », *Revue de Sciences Criminelles*, 2009, p. 273.

L. GRARD, Transfert de données personnelles des passagers, *Revue de droit des transports*, n° 9, comm. 197, septembre 2007.

P. GRECIANO, « La jurisprudence de la Cour de justice de l'Union européenne », *Revue française de linguistique appliquée*, 2014, pp. 59-70.

C. GUERRIER, « Les aspects techniques de la régulation des données personnelles : la question du numéro IP », *LEGICOM*, 2009, pp. 127-141.

E. GUILD, E. BROUWER, "The political life of data: the EJC Decision on the PNR Agreement between the EU and the US", *CEPS*, 26 juillet 2006.

E. GUISSART, J-F. HENROTTE, « Profilage : la segmentation jusque dans le régime du RGPD », *PIN CODE*, 2020, pp. 10-18.

B. HACKETT, "Covering (Up) the War on Terrorism: The Master Frame and the Media Chill", *Campaign for press & broadcasting freedom*, 2001.

C. R. HAN, R. MCGAURAN, H. NELEN, « API and PNR data in use for border control authorities », *Security Journal*, 2016.

M. H. HOFFMAN, "Rescuing the Law of War: A Way Forward in an Era of Global Terrorism", *The US Army War College Quarterly: Parameters*, Volume 35, Number 2, 2005 ; en ligne sur : <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2260&context=parameters>

L. IDOT, « Vers une Union de la sécurité », *Europe*, n° 11, alerte 57, novembre 2017.

S. IN'T VELD, *Europolitique*, n° 4409, 20 avril 2012.

J.-P. JACQUE, « Une élection de 'second ordre' ? », *Revue trimestrielle de droit européen*, 2019.

P. JANUEL, « Séparatisme : les principales dispositions de la loi », *Dalloz*, Administratif – Pénal, 7 septembre 2021, en ligne sur : <https://www.dalloz-actualite.fr/flash/separatisme-principales-dispositions-de-loi>

J. JEANDESBOZ, « Ceci n'est pas un contrôle : PNR Data Processing and the Reshaping of Borderless Travel in the Schengen Area », *European Journal of Migration and Law*, 2021, pp. 431-456.

J. JEAN-MARIE, « Transport aérien - La crise sanitaire porte un coup d'arrêt au trafic aérien INSEE », *Conjoncture Martinique*, n° 14, 08 juillet 2021.

- G. JOFFÉ, "European multilateralism and soft power projection in the Mediterranean", *Instituto da Defesa Nacional*, 2 series, n° 101, Primavera, 2002 ; en ligne sur : https://comum.rcaap.pt/bitstream/10400.26/1336/1/NeD101_GeorgeJoffe.pdf
- F. JOZEK, « Les ressources extra-aéronautiques des aéroports commerciaux », *Droit et Ville*, vol. 82, n° 2, 2016, pp. 3-18.
- B. JUANALS, « Protection des données personnelles et TIC au cœur des enjeux de société et de la mondialisation : les mécanismes d'un contrôle distribué », *tic&société*, vol. 8, n° 1-2, 1^{er} semestre 2014 et 2^e semestre 2014 ; en ligne sur : <http://journals.openedition.org/ticetsociete/1475>
- P. KANTOR, "Territory, Authority, Rights: From Medieval to Global Assemblages by Saskia Sassen", *Political Science Quarterly*, 2007 ; en ligne sur : https://www.researchgate.net/publication/259814850_Territory_Authority_Rights_From_Medieval_to_Global_Assemblages_by_Saskia_Sassen
- O. KEMPF, « Les combattants étrangers jihadistes, entre modernisme et mutation », *Revue Défense Nationale*, 2015, pp. 111-116.
- E. KESSOUS, « Le Traité de Maastricht : un coup d'État monétaire », *Vacarme*, 1997, p. 33.
- D. KORFF, M. GEORGES, "Passenger Name Records, data mining & data protection: the need for strong safeguards", *The Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data*, 2015, p. 34
- J.-C. KROSS, « État des lieux de la lutte contre le terrorisme en France », *Revue française de criminologie et de droit pénal*, n° 8, avril 2017.
- E. M. KUŞKONMAZ, "Privacy and Border Controls in the Fight against Terrorism", *Immigration and Asylum Law and Policy in Europe*, Volume 48, 18 mars 2021.
- H. LABAYLE, « Architecte ou spectatrice ? La Cour de justice de l'Union dans l'Espace de liberté, sécurité et justice », *Revue trimestrielle de droit européen*, 2006, p. 1.
- H. LABAYLE, R. MEHDI, « Terrorisme: les jours d'après », *KritV, CritQ, RCrit. Kritische Vierteljahresschrift Für Gesetzgebung Und Rechtswissenschaft, Critical Quarterly for Legislation and Law, Revue Critique Trimestrielle de Jurisprudence et de Législation*, 2015, pp. 3-7 ; en ligne sur : <http://www.jstor.org/stable/43784263>
- J. LAGASSE, « 'Fichier' PNR : surveillance électronique de masse ou nouveau paradigme de la sécurité ? », *Les Notes du CREOGN*, 2016.
- V. M. LAGRANGE, « La Cour de justice des Communautés européennes : du plan Schuman à l'Union européenne », *Revue trimestrielle de droit européen*, Dalloz, 1978.

- M. LALDJI, « Les menaces des entités criminelles transnationales sur la sécurité intérieure des États », *Sécurité globale*, 2016, pp. 43-62.
- M.-T. LANQUETIN, « Le droit de la non-discrimination en Europe », *Travail et genre dans le monde*, 2013, pp. 52-61.
- X. LATOUR, « Les fichiers PNR et les transports aériens internationaux », *Annuaire du droit de la sécurité et de la défense 2018*, Mare et Martin, 2018, pp. 247-258.
- X. LATOUR, « La participation des personnes privées au contrôle des migrations en France », *Actualité Juridique Droit Administratif*, Dalloz, 2019.
- N. LE BONNIEC, « L'Union européenne à l'ère du numérique et la lutte contre le terrorisme : la sécurité au détriment de l'État de droit avec les accords PNR ? », in « Quel État de droit dans une Europe en crise ? », *Revue des droits et libertés fondamentaux*, n° 44, Chronique, 2019 ; en ligne sur : <https://revuedlf.com/droit-ue/lunion-europeenne-a-ler-du-numerique-et-la-lutte-contre-le-terrorisme-la-securite-au-detriment-de-letat-de-droit-avec-les-accords-pnr/>
- A. LEE, A.G. NIKOLAEV, S. JACOBSON, "Protecting air transportation: a survey of operations research applications to aviation security", *Journal of Transportation Security*, 2008.
- S. LE STRUJON, « Le California Consumer Privacy Act : premier pas vers un RGPD américain ? », *Revue de l'Union européenne*, Dalloz, 2020.
- R. LEVY, « Ordre social et répression pénale, Crime et insécurité : un demi-siècle de bouleversement », CNRS, 2005 ; en ligne sur : <https://journals.openedition.org/sdt/20050>
- G. LYKOU, A. ANAGNOSTOPOULOU, D. GRITZALIS, « Smart airport cybersecurity: threat mitigation and cyber resilience controls », *Sensors* (Basel), 21 décembre 2018.
- N. MALLET-POUJOL, « Protection des données personnelles et droit à l'information », *LEGICOM*, 2017, pp. 49-59.
- S. MANACORDA, « Le droit pénal sous Lisbonne : vers un meilleur équilibre entre liberté, sécurité et justice », *Revue de Science criminelle et de droit pénal comparé*, 2010.
- F. MARIATTE, « Protection des données personnelles des usagers des transports aériens », *Nouvelles technologies*, Europe, LexisNexis, n° 7, juillet 2004.
- N. MARTIAL-BRAZ, « Le profilage, fiche pratique », *Communication Commerce électronique*, n° 4, Dossier 15, LexisNexis, avril 2018.
- A. N. MARTIN, « Américanisation ou européanisation du droit pénal économique ? », *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2006.

- F. MASSART-PIERARD, « Le Parlement européen : l'irrésistible mouvement de conquête des pouvoirs », *Revue internationale de politique comparée*, 2009, pp. 545-557 ; en ligne sur : <https://www.cairn.info/revue-internationale-de-politique-comparee-2009-4-page-545.htm>
- J. MASTERS, « Guantanamo Bay: Twenty Years of Counterterrorism and Controversy », *Council on Foreign Relations*, 5 octobre 2021 ; en ligne sur : <https://www.cfr.org/article/guantanamo-bay-twenty-years-counterterrorism-and-controversy>
- A. MATTELART, A. VITALIS, « La captation et l'exploitation marchande des identités », *Le profilage des populations*, 2014.
- E. MAUPIN, « Les libertés individuelles à l'épreuve de la sortie de crise sanitaire », *Droit fondamental et liberté publique*, Administratif, Dalloz, 6 septembre 2021 ; en ligne sur : <https://www.dalloz-actualite.fr/flash/libertes-individuelles-l-epreuve-de-sortie-de-crise-sanitaire>
- Y. MAYAUD, *Répertoire de droit pénal et de procédure pénale*, Dalloz, Terrorisme – Prévention, janvier 2018.
- V. MAYER-SCHÖNBERGER, « La révolution Big Data », *Politique étrangère*, 2014, pp. 69-81.
- L. A. MCLAY, S. H. JACOBSON, J. E. KOBZA, “The tradeoff between technology and prescreening intelligence in checked baggage screening for aviation security”, *Journal of Transportation Security*, 2008, pp. 107-126.
- J. J. MEARSHEIMER, “Bound to Fail: The Rise and Fall of the Liberal International Order”, *International Security*, pp. 7-50, 2019.
- E. MECHOULAN, « Faut-il créer une agence de renseignement européenne ? », *Politique étrangère*, 2019, pp. 125-139 ; en ligne sur : <https://www.cairn.info/revue-politique-etrangere-2019-4-page-125.htm?ref=doi>
- A. MÉGIE, « Généalogie du champ de la coopération judiciaire européenne », *Cultures & Conflits*, L'Harmattan, n° 62, 2006.
- F. MÉGRET, “‘War’? Legal Semantics and the Move to Violence,” *European Journal of International Law*, 2002, p. 361.
- A. MENON, « La politique de défense européenne après le Traité de Lisbonne, beaucoup de bruit pour rien », *Politique étrangère*, 2011, pp. 375-387.
- B. MERCADAL, « Aviation », *Répertoire de droit commercial*, Dalloz, novembre 2017.
- C. MESTRE, « Conseil de l'Union européenne », *Répertoire de droit européen*, Dalloz, octobre 2021.

- V. MICHEL, La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration, *La revue trimestrielle de droit européen*, Dalloz, n° 3, 2006, pp. 549-559.
- T. MINSEN, C. SEITZ, M. ABOY, M. C. COMPAGNUCCI, « The EU-US Privacy Shield Regime for Cross- Border Transfers of Personal Data under the GDPR », *Lexxion*, 2020.
- V. MITSILEGAS, « Contrôle des étrangers, des passagers, des citoyens : surveillance et anti-terrorisme », *Cultures & conflits*, 60, 2005.
- J. MONAR, « La mise en œuvre de l'espace de liberté, de sécurité et de justice : un défi pour l'Union européenne et pour les États membres », *Revue française d'administration publique*, 2009, pp. 15-34.
- R. MORGAN, "The Rule of Law. By Tom Bingham", *The British Journal of Criminology*, Volume 50, Issue 6, November 2010, pp. 1202-1205.
- J. MORAND-DEVILLER, « Le territoire fiction », *Actualité juridique droit administratif*, Dalloz, 2000, p.1461.
- E. MUIR, « L'action juridique de l'Union européenne dans la lutte contre les discriminations », *Migrations société*, 2010, pp. 87-104.
- M.-C. NAVES, « Entre unilatéralisme et dénégation, la gestion de la crise du Covid-19 selon Donald Trump », *IRIS*, 17 avril 2020 ; en ligne sur : <https://www.iris-france.org/146292-entre-unilateralisme-et-denegation-la-gestion-de-la-crise-du-covid-19-selon-donald-trump/>
- S. NAWAF SHATHIL, « L'utilisation des données personnelles dans la lutte contre le terrorisme », *International Journal of Open Governments*, Les Editions IMODEV, vol 5, 2019.
- D. NAZET ALLOUCHE, « Politique sociale – acteurs », *Répertoire de droit européen*, Dalloz, 2019.
- B. NIVET, « De Maastricht à Nice : la laborieuse ascension de l'Union européenne », *Revue internationale et stratégique*, 2001, pp. 135-142.
- J. NOCETTI, « Géopolitique de la cyber-conflictualité », *Politique étrangère*, n° 2, 2018, pp. 15-27.
- F. NWAMEN, « Impact des technologies de l'information et de la communication sur la performance commerciale des entreprises », *La Revue des Sciences de Gestion*, vol. 218, n° 2, 2006, pp. 111-121.
- L. OBADIA, « Technologies mondialisées, mondialisation technologique, Digital Globalization : quels liens entre les NTIC et la mondialisation ? », *Diogène*, vol. 271-272, n° 3-4, 2020, pp. 110-132.

- J.-C. PAILLÈS, « Les systèmes de paiement électronique sur internet », *Les cahiers du numérique*, 2003, pp. 45-69.
- S. PARIER, « Les incidences de la privatisation sur les usagers : entre faux-semblants et réalités », *Juris tourisme*, Tourisme & territoire, Aéroports, Dalloz, n° 206, 2018.
- S. PARIER, « Privatisation : un projet « révolutionnaire » ? », *Juris Tourisme*, Tourisme & territoire, Aéroports de Paris, Dalloz, n° 214, 2018.
- S. PARIER, « L'action de groupe et le RGPD en matière de transport aérien », *Juris tourisme*, Dalloz, 2019, n° 215.
- J.-C. PAYE, « Lutte antiterroriste et contrôle de la vie privée », *Multitudes*, 2003, pp. 91-105 ; en ligne sur : <https://www.cairn.info/revue-multitudes-2003-1-page-91.htm>
- B. PELLEGRINI, « Logique préventive et droit des libertés publiques », *La revue lacanienne*, 2007, pp. 82-85.
- S. PEYROU, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », *Droits fondamentaux, Europe, Revue Mensuelle LexisNexis Jurisclasseur*, juillet 2012.
- S. PEYROU-BARTOLL, « Nouvelles technologies, sécurité et protection des données à caractère personnel : un cadre juridique européen à la hauteur des enjeux ? », *Cahiers de la sécurité et de la justice*, 2022, pp.186-196.
- S. PEYROU-PISTOULEY, « Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer: réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne », *Europe actualité du droit communautaire*, 2012.
- F. PIERRU, « Introduction. L'administration hospitalière, entre pandémie virale et épidémie de réformes », *Revue française d'administration publique*, vol. 174, n° 2, 2020, pp. 301-315 ; en ligne sur : <https://doi.org/10.3917/rfap.174.0005>
- A. PLAW, "Targeting Terrorists. A Licence to Kill?", *Aldershot*, Ashgate, 2008.
- J.-M. PONTIER, « Territorialisation et déterritorialisation de l'action publique », *AJDA*, 1997.
- P. PONZANO, « Le droit d'initiative législative de la Commission européenne : théorie et pratique », *Revue des affaires européennes*, n° 1, 2009.
- J.-M. POTTIER, « Polycrise », *Sciences humaines*, Actualité de la recherche, mensuel n° 358, mai 2023.
- R. POZNANSKI, « Le fichage des juifs de France pendant la Seconde Guerre mondiale et l'affaire du fichier des juifs », *Gazette des archives*, 1997, pp. 250-270.

- M. PRIVAL, « L'accord PNR approuvé sans grand engouement par le Parlement européen », *Le Taurillon*, 2012 ; en ligne sur : <https://www.taurillon.org/L-accord-PNR-approuve-sans-grand-engouement-par-le-Parlement-europeen,04947>
- K. PROPP, “Avoiding the Next Transatlantic Security Crisis: The Looming Clash Over Passenger Name Record Data”, *Atlantic Council*, 2021 ; en ligne sur : https://www.atlanticcouncil.org/wp-content/uploads/2021/07/Avoiding-the-Next-Transatlantic-Security-Crisis-The-Looming-Clash-over-Passenger-Name-Record-Data_Final.pdf
- C. RAFFESTIN, & M. BRESSO, « Tradition, modernité, territorialité », *Cahiers de géographie du Québec*, 1982, en ligne à URL : <https://doi.org/10.7202/021557ar> consulté le 20 juillet 2023.
- D. RAMIREZ, J. HOOPES, ET T. LAI QUINLAN, “Defining Racial Profiling in a PostSeptember 11 World”, *American Criminal Law Review*, vol. 40, 2003, pp. 1195-1233.
- T. S. RENOUX, « Juger le terrorisme ? », *Cahiers du Conseil constitutionnel*, n° 14, Dossier : La Justice dans la Constitution, mai 2003 ; en ligne sur : <https://www.conseil-constitutionnel.fr/node/2915/pdf>
- M. RICH, “Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment”, *University of Pennsylvania Law Review*, 2016 ; en ligne sur : <http://ssrn.com/abstract=2593795>
- P. RODIÈRE, « Sécurité sociale - Droit de l'Union européenne », *Répertoire de droit international*, Dalloz, avril 2019.
- S. RODOTA, « Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives », *Mouvements*, vol. 62, n° 2, 2010, pp. 55-70.
- S. RODRIGUES, « Transports aériens », *Répertoire de droit européen*, Dalloz, 2018.
- J.-L. RONGÉ, « Déchéance : à propos du projet de révision constitutionnelle concernant les binationaux condamnés pour terrorisme - Du sentiment renforcé d'être différent », *Journal du droit des jeunes*, n° 350, 2015, pp. 9-17.
- S. ROUSSEL, P. JANURA, « Les relations canado-européennes en matière de sécurité : Nouveau contexte et nouveaux enjeux pour l'UE et le Canada », *Note de recherche*, Centre d'études sur l'intégration et la mondialisation, Université du Québec à Montréal, 2002.
- J. RULE, « La protection des données personnelles aux États-Unis : la réaction à la directive européenne », *Revue française d'administration publique*, janvier-mars 1999.

- D. SABBAGH, « Sécurité et libertés aux États-Unis dans l'après-11 septembre : un état des lieux », *Critique internationale*, n° 19, 2003, pp. 17-23 ; en ligne sur : <https://www.cairn.info/revue-critique-internationale-2003-2-page-17.htm>
- J.-M. SAUVÉ, « Le principe de proportionnalité, protecteur des libertés ? », *Les cahiers Portalis*, 2018, pp. 9-21.
- P. J. SCHRAEDER, « La guerre contre le terrorisme et la politique américaine en Afrique », *Politique africaine*, n° 98, 2005, pp. 42-62.
- S. SERVERIN, « La légitimité de la Constitution dans la doctrine constitutionnelle japonaise », *Mémoires et responsabilités de guerre. Les procès de Tôkyô et de La Haye*, *Droit et cultures*, 2009, pp. 179-198 ; en ligne sur : <http://journals.openedition.org/droitcultures/2191>
- J. SHANE, « Air transport in crisis », *Revue de droit des transports*, n° 12, entretien 1, décembre 2008.
- A. SCHERRER, A. MEGIE, V. MITSILEGAS, « La stratégie de l'Union européenne contre la criminalité organisée : entre lacunes et inquiétudes », *Cultures & Conflits*, n° 74, été 2009, 28 octobre 2010 ; en ligne sur : <http://journals.openedition.org/conflits/17442>
- D. SIMON, « Droit fondamentaux », *Europe*, Commentaire n° 345, octobre 2017, pp. 17-18.
- G. A. SINHA, « NSA surveillance since 9/11 and the human right to privacy », *Loyola Law Review*, 2013 ; en ligne sur : <https://dspace.loyno.edu/jspui/bitstream/123456789/121/1/Sinha.pdf>
- B. STIRN, « Europe et droits fondamentaux », *Le Grand Continent*, 6 novembre, 2019 ; en ligne sur : <https://legrandcontinent.eu/fr/2019/11/06/europe-et-droits-fondamentaux/>
- B. STIRN, « L'indépendance du juge dans le cadre européen : évolutions et interrogations partagées », *Revue trimestrielle des droits de l'Homme*, n° 125, 2021, pp. 5-13.
- H. SURREL, « La protection des données à caractère personnel, domaine emblématique des interactions jurisprudentielles entre cours européennes et Conseil constitutionnel », *Titre VII*, 2019/1, 2019 ; en ligne sur : https://www.cairn.info/article.php?ID_ARTICLE=TVII_002_0051
- B. TARABAY, « L'opposabilité des droits fondamentaux dans les pays arabes », *Campus international*, 2017, en ligne sur : <https://avocatcampusinternational.org/accueil-liban/images/presse/Opposabilite-des-droits-fondamentaux-dans-les-pays-arabes.pdf>
- M. TERRACOL, « Quel est le rôle de la Ligue arabe ? », *GEO*, 5 octobre 2022 ; en ligne sur : <https://www.geo.fr/geopolitique/quel-est-le-role-de-la-ligue-arabe-211898>

- E. THELISSON, « La portée du caractère extraterritorial du Règlement sur la protection des données », *Revue internationale de droit économique*, Association internationale de droit économique, pp. 501-533 ; en ligne sur : <https://www.cairn.info/revue-internationale-de-droit-economique-2019-4-page-501.htm>
- B. THÉRET, “The New EU Social Policies in the Light of the Canadian Experience of Federalism”, *Sociétés contemporaines*, 2002, pp. 51-78.
- H. THERY, « Mondialisation, déterritorialisation, reterritorialisation », *Bulletin de l'Association de Géographes Français*, vol. 85-3, 2008, pp. 324-331.
- N. TILLI, La protection des données à caractère personnel, *Documentaliste-Sciences de l'information*, 2013, pp. 62-69.
- R. TINIERE, « L'influence croissante de la Charte des droits fondamentaux sur la politique extérieure de l'Union européenne », *Revue des droits et libertés fondamentaux*, 2018.
- J. VALERO TORRIJOS & M. ANDREU MARTINEZ, « L'encadrement juridique des données ouvertes en Espagne », *Revue française d'administration publique*, 2018/3 N°167, pp.601-611.
- J. TRICOT, « Droit et jurisprudence de l'UE », *Revue de science criminelle et de droit pénal comparé*, 2018, pp. 203-228.
- M. TSAYEM DEMAZE, « Quête de justice climatique et reconfiguration de la lutte contre les changements climatiques en marge des COP », *L'Information géographique*, vol. 87, n° 3, 2023, pp. 25-47.
- K. TUORI, « Vers une théorie du droit transnational », *Revue internationale de droit économique*, 2013, pp. 9-36.
- A. TÜRK, P. PIAZZA, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée, Entretien avec Alex TÜRK ; propos recueillis par Pierre PIAZZA », *Cultures & Conflits*, 2004, pp. 115-134.
- D. VAN PUYVELDE, « Sécurité de l'information et partenariats public-privé dans le renseignement américain », *Sécurité et stratégie*, 2014, pp. 25-30 ; en ligne sur : <https://www.cairn.info/revue-securite-et-strategie-2014-2-page-25.htm>
- F. VINDEVOGEL, « La remise en question des politiques pénales ultra-répressives : tendance lourde ou évolution conjoncturelle ? », *Revue française d'études américaines*, 2007/3 (n° 113), 2007, pp. 92-107.
- S. VON SOLMS, R. VAN HEERDEN, “The consequences of Edward Snowden NSA related information disclosures”, Conference: 10th International conference on Cyber Warfare and Security ICCWS, Sukuza, South Africa, 2015 ; en ligne sur :

<https://www.researchgate.net/publication/275019554> The Consequences of Edward Snowd en NSA Related Information Disclosures

A. WAGENER, « Réactions post-attentats en France et en Belgique : étude comparative des discours de l'exécutif politique », *Mots. Les langages du politique*, n° 116, 2018, pp.111-130.

K. WAHL-JORGENSEN, L. BENNETT, G. TAYLOR, « The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Revelations », *International journal of communication*, Cardiff University, UK, 2017, pp. 740-762 ; en ligne sur : <https://dspace.loyno.edu/jspui/bitstream/123456789/121/1/Sinha.pdf>

W. H. WARE, « Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security », *RAND Report R-609-1*, octobre 1979.

S. A. WARREN, «Data Privacy Protection in the Region and Worldwide: Stakes and Challenges», *The MENA Business Law Review*, LexisNexis, 2018.

S. A. WARREN, « Staying on top of data privacy », *India Business Law Journal, Ikigai Law*, 22 mars 2023 ; en ligne sur : <https://law.asia/data-protection-laws/>

M.-A. WEISS, « De la sphère au bouclier : qu'est-ce que le Privacy Shield ? », *I2D - Information, données & documents*, 2016/3 (Volume 53), pp. 20-22 ; en ligne sur : <https://www.cairn.info/revue-i2d-information-donnees-et-documents-2016-3-page-20.htm>

C. WIHTOL DE WENDEN, J. DRAVIGNY, « Soixante ans après le Traité de Rome : regards sur la liberté de circulation en Europe », *Migrations société*, 2019, pp. 17-29.

G. ZIGNANI, « Protection des données : le législateur appelé à intervenir rapidement », *La Gazette des communes*, 15 mars 2017.

« Coronavirus (Covid-19) : les rappels de la CNIL sur la collecte de données personnelles », *Revue Lamy Droit de l'immatériel*, n° 169, 1^{er} avril 2020.

« Ordre public », *Droit administratif*, Dalloz, septembre 2021.

4. CONTRIBUTIONS À DES OUVRAGES COLLECTIFS

J. AUVRET-FINCK, « L'échange d'information dans les accords PNR conclus par l'Union européenne avec des États tiers », in C. Chevallier-Govers (dir.), *L'échange des données dans l'espace de liberté, de sécurité et de justice de l'Union européenne*, Mare & Martin, coll. « Droit public », 2017.

C. BERTRAM, « Notre guerre contre le terrorisme », in *Justifier la guerre*, Presses de Science Po, 2013, pp. 221-238.

- D. BIGO, L. BONELLI, T. DELTOMBE, « Les libertés sacrifiées au nom de la sécurité ? », Introduction, in *Au nom du 11 septembre... Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, 2008.
- I. BOUHADANA, W. GILLES, « Introduction – cyberspace, cybercriminalité & libertés », in I. Bouhadana, W. Gilles (dir.), *Cybercriminalité, cybermenaces & cyberfraudes*, Les éditions IMOD-V, mars 2012.
- I. BOUHADANA, W. GILLES, J. HARIVEL, “Freedom of expression and the values of the French Republic. Article dedicated to the memory of the victims of the terrorist attacks of 2015 in France”, in Russell L. Weaver, Steven I. Friedland (eds.), *Comparative Perspectives on Freedom of Expression*, Global Papers Series, Vol. II, Carolina Academic Press, 2017, pp. 141-158.
- R. CARTER, « Chapitre premier. Les transports aériens : un risque identifié, une menace globalisée », in Raymond H. A. Carter, *La sûreté des transports. Les transports face aux risques et menaces terroristes*, PUF, 2008, pp. 13-109.
- C. CHIAMBARETTO, E. COMBE, « L'écosystème du transport aérien et sa régulation », in *Le transport aérien*, La Découverte, 2023, pp. 29-56.
- P. CHIAMBARETTO, E. COMBE, « V / Les défis à venir du transport aérien », in Paul Chiambaretto (dir.), *Le transport aérien*, La Découverte, 2023, pp. 99-118.
- J.-M. DEFAYS, « Harmoniser les cultures, orchestrer la communication dans la classe et en dehors », *Mardaga*, PSY-Théories, débats, synthèses, in *Enseigner le français – Langue étrangère et seconde, approche humaniste de la didactique des langues et des cultures*, 2018.
- C. DE TERWANGNE, K. ROSIER (dir.), « Des lignes directrices du Groupe de l'article 29 aux travaux (futurs) du Comité européen de la protection des données (CEPD) in *Le règlement général sur la protection des données (RGPD, GDPR)*, Larcier, 2018.
- J. EYNARD, « Quelle définition pour un régime de protection efficace ? », in *Les données personnelles*, Michalon, 2013, pp. 109-132.
- G. FERRAGU, « En rouge et noir, une génération en guerre civile », in *Histoire du terrorisme*, Perrin, 2014, pp. 376-428.
- O. H. GANDY, “Data mining, surveillance, and discrimination in the post-9/11 environment”, in K. Haggerty, R. Ericson (eds.), *The new politics of surveillance and visibility*, University of Toronto Press, 2006, pp. 363-384.
- V. GAUTRON, D. MONNIAUX, « De la surveillance secrète à la prédiction des risques : les dérives du fichage dans le champ de la lutte contre le terrorisme », in *Archives de politique criminelle*, Terrorisme, Éditions Pédone, 2016, pp. 123-135.

- G. HOUCHON, « Les peines incompressibles », in *Pénologie, science sociale, Médecine et hygiène*, 2021, pp. 65-89.
- X. LATOUR, « La sécurité privée ou l'État autrement », in P. Brajeux, E. Delbecq et M. Mathieu (dir.), *Sécurité privée, enjeu public*, Armand Colin, 2013, p. 215.
- L. A. MCLAY, "Risk-Based Resource Allocation Models for Aviation Security", in *Safety and Risk Modeling and Its Applications*, Springer, 2011, pp. 243-261.
- A. MATTELART, « La guerre sans fin, le paradigme techno-sécuritaire », in *La Globalisation de la surveillance*, La Découverte, 2008, pp.166-192.
- R. McMASTER, « La pandémie de Covid-19 en Écosse et au Royaume-Uni, entre "déficits" de soins et solidarité », *Revue française de socio-économie*, 2021/1, n° 26, 2021.
- F. MICHEA, « Les finalités des systèmes d'information européens à vocation migratoire », l'Union européenne et la tentation du panoptique, in S. Turgis, *Les données numériques des migrants et des réfugiés sous l'angle du droit européen*, Presses universitaires de Rennes, 2020, pp. 37-63.
- J. MONAR, « The European Union's Role in the Fight against International Terrorism: An Evaluation in the Light of the Response to 11 September 2001 », in Georges Vandersanden, Aline de Walsche (dir.), *Mélanges en hommage à Jean-Victor Louis*, Institut d'études européennes, Bruxelles, éd. de l'Université de Bruxelles, Bruxelles, vol. 1, 2003, pp. 335-354.
- H. MOUTOUH, J. POIROT, « PNR (Passenger Name Record) », in *Dictionnaire du renseignement*, Perrin, 2018.
- A.-M. OLIVA, « Les agences de l'Union européenne », in *Les indispensables du droit des institutions européennes*, Ellipses, 2016, pp. 178-183.
- S. PEYROU, « La protection des données personnelles face aux programmes PNR. Une illustration du difficile équilibre entre lutte contre le terrorisme et protection des droits fondamentaux », in *Mélanges en l'honneur du Professeur Pierre Bon*, Dalloz, 2014, p. 487.
- J. POIROT, « PNR (Passenger Name Record) », in *Dictionnaire du renseignement*, 2018, pp. 611-613.
- C. RAPOPORT, « Nationalité et citoyenneté de l'Union européenne », in *La nationalité au carrefour des droits*, Presses universitaires de Rennes, 2019, pp. 89-103
- R. ROBERT, « Le Comité européen de la protection des données : le garant d'un nouvel ordre ? », in *Le règlement général sur la protection des données*, Dalloz, 2018.
- R. SEROUSSI, « Le droit japonais », in *Introduction au droit comparé*, Dunod, 2009, pp. 173-181.

R. TINIÈRE, « Droits fondamentaux et exception en droit de l'UE : dialectique entre intégration et désintégration », in *L'exception en droit de l'Union européenne*, 2019, pp. 337-346

F. TREGUER, « Surveillance numérique », in *Le Nouveau Monde : Tableau de la France néolibérale*, Éditions Amsterdam, 2021.

P. VAN DIJK, « Access to Court », in R.S.J. Macdonald *et al.*, *The European System of Protection of Human Rights*, Kluwer, 1993, pp. 345-373.

F. VERGNIOLE DE CHANTAL, « Les checks and balances à l'épreuve », in *L'impossible Présidence impériale. Le contrôle législatif aux États-Unis*, CNRS Éditions, 2016 ; en ligne sur : <http://books.openedition.org/editionscnrs/13531>

D. YOUNG, « Vers un nouveau droit pénal des mineurs », in *Juger et éduquer les mineurs délinquants*, Dunod, 2009, pp. 103-118.

5. RAPPORTS ET ÉTUDES

Gouvernement, *Rapport sur le maillage aéroportuaire français*, Conseil supérieur de l'aviation civile, 2017.

Académie de l'Air et de l'Espace, *Automatisation des avions de transport à l'horizon 2050*, Étude, Aviation plus automatique, interconnectée, à l'horizon 2050, Commission aéronautique civile, Dossier n° 42, 2018, en ligne sur : <https://academieairespace.com/wp-content/uploads/2018/07/Les-Livrets-Web.pdf>

Assemblée nationale, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi, Rapport n° 2615, *Le projet de loi, après déclaration d'urgence, relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, présenté par M. Alain Marsaud, 22 novembre 2005.

Assemblée nationale, Commission des affaires européennes, *Rapport d'information sur la proposition de directive relative à l'utilisation des données des dossiers 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*, présenté par M. G. Geoffroy, 16 novembre 2011.

Assemblée nationale, Sénat, Audition, Rapport n° 3524-423, *Délégation parlementaire au renseignement relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2015*, présenté par M. J.-P. Raffarin, 25 février 2016.

Assemblée nationale, Commission des affaires étrangères et de la commission des finances, Rapport n° 4082, *Rapport d'information en conclusion des travaux d'une mission d'information constituée le 3 février 2016 sur l'extraterritorialité de la législation américaine*, présenté par Mme K. Berger, 5 octobre 2016.

Banque de France, *Rapport sur l'extraterritorialité du droit de l'Union européenne*, Haut comité juridique de la place financière de Paris, mai 2022 ; en ligne sur : https://www.banque-france.fr/sites/default/files/rapport_46_f.pdf

Conseil de l'Union européenne, *Stratégie européenne de sécurité – Une Europe sûre dans un monde meilleur*, 2009, p. 43 ; en ligne sur : <https://www.consilium.europa.eu/media/30810/qc7809568frc.pdf>

Cour des comptes, *Le processus de privatisation des aéroports de Toulouse, Lyon et Nice*, Communication à la commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale, octobre 2018 ; en ligne sur : <https://www.ccomptes.fr/system/files/2018-11/20181113-processus-privatisation-aeroports-Toulouse-Lyon-Nice.pdf>

Direction générale de l'Aviation civile, *Activités liées aux aéroports à l'horizon 2025*, Les notes d'analyse de la DGAC, Éclairages, septembre 2017, n° 3 ; en ligne sur : https://www.ecologie.gouv.fr/sites/default/files/Eclairage_n_3_VF_web.pdf

European Union Agency for Network and Information Security, *Securing Smart Airport*, 2016.

Government Accountability Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges* 5-6, Rapport GAO-04-385, février, 2004.

House of Lords, *The EU/US Passenger Name Record (PNR) Agreement*, European Union Committee, 5 juin 2007 ; en ligne sur : <https://publications.parliament.uk/pa/ld200607/ldselect/ldeucom/108/108.pdf>

Human Rights Watch, *The Road to Abu Ghraib*, IV. Iraq: Applying Counter-Terrorism Tactics during a Military Occupation, 8 juin 2014.

IATA, *Annual review*, 2013 ; en ligne sur : <https://www.iata.org/contentassets/c81222d96c9a4e0bb4ff6ced0126f0bb/iata-annual-review-2013-en.pdf>

Ministère de l'Intérieur, *Le livre blanc de la sécurité intérieure*, 2020.

National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, Authorized ed. (New York, W.W Norton & Co., 2004).

Sénat, Commission des lois, Rapport n° 401, *La proposition de décision-cadre relative à l'utilisation de données des dossiers passagers à des fins répressives*, présenté par M. Simon Sutour et M. Yves Détraigne, 13 mai 2009.

Transportation Research Board Airport, *A primer to prepare for the connected airport and the internet of things*, Report 19, Cooperative Research Program (ACRP), 2019.

US Department of Homeland Security, *A Report On The Use And Transfer Of Passenger Name Records Between The European Union And The United States*, 26 juin 2015 ; en ligne sur :

https://www.dhs.gov/sites/default/files/publications/privacy_pcr_pnr_review_06262015.pdf

White House Commission on Aviation Safety and Security, *Final Report to President Clinton*, 12 février, 1997.

6. WEBOGRAPHIE

ACLU, The four biggest problems with the "secure flight" airline security program, 2005, en ligne à URL : <https://www.aclu.org/documents/four-biggest-problems-secure-flight-airline-security-program> consulté le 24 juillet 2023.

Aéroport de Lyon, Politique de protection des données, 9 juillet 2020, en ligne à URL : https://www.lyonaeroports.com/sites/default/files/2020-07/politique_donnees_personnelles_20200709.pdf consulté le 20 juillet 2023.

AFTM, « Le parcours de la donnée : PNR et voyage des données », Récolte – Législation et protection des données, *Données : de la récolte à la valorisation*, Fiche 14, août 2017, en ligne à URL : https://www.aftm.fr/wp-content/uploads/2017/08/Fiche-14_PNR_et_voyage_des_donnees_LB-AFTM2017.pdf consulté le 16 juillet 2023.

Air Transat, « Aéroport de Bruxelles : Nouvelles mesures de sécurité », en ligne à URL : <https://www.airtransat.com/fr-CA/nouvelles/archives/aeroport-de-bruxelles-avis-de-voyage> consulté le 8 juin 2023.

AMELI, « Épidémie, pandémie, gestion sanitaire : ce qu'il faut savoir », *Santé*, 21 juin 2023, en ligne à URL : <https://www.ameli.fr/assure/sante/themes/epidemie-et-pandemie/epidemie-et-pandemie-quelle-difference#:~:text=C'est%20le%20cas%20par,est%20d%C3%A9finie%20comme%20une%20pand%C3%A9mie%20> consulté le 24 juillet 2023.

American Civil Liberties Union, “The Five Problems With CAPPS II: Why the Airline Passenger Profiling Proposal Should Be Abandoned”, 2004, en ligne à URL :

<https://ics.uci.edu/~redmiles/ics131-FQ03/week03privacy/CAPPS2.pdf> consulté le 13 décembre 2023.

R.-P. ANDLAUER, « Nouvelle série de privatisations concernant Aéroport de Paris, Française des Jeux et Engie », *CVS Avocats*, Droit des sociétés, 5 septembre 2018, en ligne à URL : https://www.cvs-avocats.com/uploads/media/media/5e68ca2d5128f_option-droit-affaires-nouvelle-se-rie-de-privatisations-concernant-aeroport-de-paris-francaise-des-jeux-et-engie-rene-pierre-andlauer.pdf consulté le 29 juin 2023.

L. ASGARALI, « L'arsenal technologique de la Chine pour lutter contre le coronavirus », *Le Figaro*, Tech & web, 17 février 2020, en ligne à URL : <https://www.lefigaro.fr/secteur/high-tech/detecteur-de-chaleur-corporelle-drones-la-chine-recourt-massivement-aux-technologies-pour-contenir-le-coronavirus-20200207> consulté le 20 juillet 2023.

A. AUTIN, « Voici la meilleure compagnie aérienne du monde en business class (ce n'est pas Air France ni Singapour Airlines) », *GQ Magazine*, 13 décembre 2023, en ligne à URL : <https://www.gqmagazine.fr/article/meilleure-compagnie-aerienne-du-monde-en-business-class-qatar-airways-et-pas-air-france-ni-singapour-airlines> consulté le 21 janvier 2024.

F. BAJAK, K. CHAN, « Biden order promises EU citizens better data privacy », *AP NEWS*, 7 octobre 2022, en ligne à URL : <https://apnews.com/article/biden-technology-data-privacy-ursula-von-der-leyen-european-commission-493ea47a4991b0c933bea2bbb47c2c6c> consulté en ligne le 14 juin 2023.

S. BASCOU, « Comment l'Europe a abandonné vos données personnelles aux espions américains », *01net*, Politique, Droits, 2 juillet 2023, en ligne à URL : <https://www.01net.com/actualites/comment-leurope-a-abandonne-vos-donnees-personnelles-aux-espions-americaains.html> consulté le 22 août 2023.

B. BAYART, « Aéroports de Paris : l'État prépare la privatisation », *Le Figaro*, 8 décembre 2017, en ligne à URL : <https://www.lefigaro.fr/societes/2017/12/08/20005-20171208ARTFIG00289-aeroports-de-paris-l-etat-prepare-la-privatisation.php> consulté le 8 mai 2023.

M.-V. BERNARD, « 'N'importe qui peut être arrêté' : à Hong Kong, la Chine a réduit la société civile au silence », *France info*, 1^{er} juillet 2022, en ligne à URL : https://www.francetvinfo.fr/monde/chine/hong-kong/n-importe-qui-peut-etre-arrete-a-hong-kong-la-chine-a-reduit-la-societe-civile-au-silence_5226565.html consulté le 24 juillet 2023.

T. BERTHEMET, « Edward Snowden, l'homme qui fait trembler le gouvernement américain », *Le Figaro*, 10 juin 2013, en ligne à URL :

<https://www.lefigaro.fr/international/2013/06/10/01003-20130610ARTFIG00394-etats-unis-edward-snowden-un-whistleblower-contre-la-nsa.php> consulté le 6 juillet 2023.

G. BESNIER, « Le règlement général sur la protection des données personnelles : symbole d'une Europe qui protège », *Le Taurillon*, 28 mai 2018, en ligne à URL : <https://www.taurillon.org/le-reglement-general-sur-la-protection-des-donnees-personnelles-symbole-d> consulté le 12 novembre 2021.

BfDI, "Instructions for using the Ehteraz and Hayya apps", 15 novembre 2022, en ligne à URL : https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2022/22_Ehteraz-Hayya.html consulté en ligne le 22 mars 2023.

J. BOUISSOU, « La pandémie de Covid-19 accroît l'extrême pauvreté dans les pays les plus fragiles », *Le Monde*, 3 décembre 2020, en ligne à URL : https://www.lemonde.fr/economie/article/2020/12/03/la-pandemie-de-covid-19-accroit-l-extreme-pauvrete-dans-les-pays-les-plus-fragiles_6062005_3234.html consulté le 24 juillet 2023.

V. BRENGARTH, « Le procès des attentats du 13 novembre est symptomatique des déficiences de la justice antiterroriste », *Le Monde*, 25 juillet 2022, en ligne à URL : https://www.lemonde.fr/idees/article/2022/07/25/le-proces-des-attentats-du-13-novembre-est-symptomatique-des-deficiences-de-la-justice-antiterroriste_6136004_3232.html consulté le 25 juillet 2023.

Bureau européen de Bruxelles, « Un code couleur pour cibler les passagers "à risques" », *Le Monde*, 21 juin 2004.

U. BUX, M. MACIEJEWSKI, « La protection des données à caractère personnel », *Fiches thématiques sur l'Union européenne*, Parlement européen, juin 2022 ; en ligne sur : <https://www.europarl.europa.eu/factsheets/fr/sheet/157/la-protection-des-donnees-a-caractere-personnel>

J. CAI, "Young and out of a job in China: how Covid-19 is creating an unemployment crisis", *South China Morning Post*, 14 octobre 2022, en ligne à URL : <https://www.scmp.com/news/china/politics/article/3190569/young-and-out-job-china-how-covid-19-creating-unemployment> consulté le 24 juillet 2023.

P. CARSTENSEN, "The Lamppost, the Wizard, and the Law: Reflections on Professor Barnett's Assessment of CAPPS II", *Risk Analysis*, 2004, en ligne à URL : https://www.researchgate.net/publication/8355955_The_Lamppost_the_Wizard_and_the_La_w_Reflections_on_Professor_Barnett's_Assessment_of_CAPPS_II consulté le 25 juillet 2023.

B. CAZENEUVE, « La directive Passenger Name Record (PNR) a été adoptée par le Parlement européen le 14 avril 2016 », *Ministre de l'intérieur*, Communiqué de presse, 14 avril 2016, en ligne à URL : <https://www.interieur.gouv.fr/Archives/Archives-des-communiques-de-presse/2016-Communiques/Adoption-du-PNR-par-le-Parlement-europeen> consulté le 23 août 2023.

L. CHECOLA, « L'UE approuve le transfert aux USA des données des passagers européens », *Le Monde*, 19 avril 2012, en ligne à URL : https://www.lemonde.fr/technologies/article/2012/04/19/le-parlement-europeen-accepte-le-transfert-aux-usa-des-donnees-de-ses-passagers_1687268_651865.html consulté le 23 avril 2023.

J. CHEMINAT, « USA et UE signent un accord pour succéder au Privacy Shield », *Le monde informatique*, 28 mars 2022, en ligne à URL : <https://www.lemondeinformatique.fr/actualites/lire-usa-et-ue-signent-un-accord-pour-succeder-au-privacy-shield-86255.html> consulté en ligne le 29 mars 2023.

China Airlines, « Privacy Protection », 31 mai 2022, en ligne à URL : <https://www.china-airlines.com/us/en/terms-and-conditions/privacy-protection> consulté en ligne le 22 mars 2023.

CJUE, Communiqué de presse n° 89/16, Conclusions de l'avocat général dans la demande d'avis 1/15, Luxembourg, le 8 septembre 2016.

Coulisses de Bruxelles, 2015, « PNR: un fichier des voyageurs aériens inutile », 21 décembre 2015.

H. CLIFTON, "Coverage focuses on criticism – not creation – of CAPPS II", *PRWeek*, 21 avril 2003, en ligne à URL : <https://www.prweek.com/article/1248561/media-watch-coverage-focuses-criticism-not-creation-capps-ii> consulté le 10 janvier 2023.

CNIL, Le « système API-PNR France », Les grands fichiers en fiches, 10 août 2016, en ligne à URL : <https://www.cnil.fr/fr/le-systeme-api-pnr-france> consulté le 10 mai 2023.

CNIL, « Traitement de données de santé : comment informer les personnes concernées ? », 4 avril 2018, en ligne à URL : <https://www.cnil.fr/fr/traitement-de-donnees-de-sante-comment-informer-les-personnes-concernees> consulté le 25 juillet 2023.

CNIL, « Qu'est-ce qu'une donnée de santé ? », 2018, en ligne à URL : <https://www.cnil.fr/fr/quest-ce-que-une-donnee-de-sante> consulté le 25 juillet 2023.

CNIL, « Quelles formalités pour les traitements de données de santé à caractère personnel ? », 8 janvier 2018, en ligne à URL : <https://www.cnil.fr/fr/applications-mobiles-en-sante-et-protection-des-donnees-personnelles-les-questions-se-poser>

CNIL, « Reconnaissance faciale dans les aéroports : quels enjeux et quels grands principes à respecter ? », 9 octobre 2020, en ligne à URL : <https://www.cnil.fr/fr/reconnaissance-faciale-dans-les-aeroports-quels-enjeux-et-quels-grands-principes-respecter> consulté le 8 juin 2023.

CNIL, « Cybersécurité : l'autorité britannique de protection des données, en coopération avec la CNIL, inflige deux amendes record », 2 novembre 2020, en ligne à URL : <https://www.cnil.fr/fr/cybersecurite-ico-en-cooperation-avec-la-cnil-inflige-amendes-record> consulté le 20 juillet 2023.

CNIL, « La CNIL précise les garanties que doit respecter la fonctionnalité TousAntiCovid-Carnet », *Dossier Covid-19*, 22 avril 2021, en ligne à URL : <https://www.cnil.fr/fr/la-cnil-precise-les-garanties-que-doit-respecter-la-fonctionnalite-tousanticovid-carnet> consulté le 23 juillet 2023.

CNIL, « Présentation de l'arrêt de la CJUE », 23 juin 2021, en ligne à URL : <https://www.cnil.fr/fr/presentation-de-larret-de-la-cjue> consulté le 30 juin 2023.

CNIL, Déclaration 01/2022 du Comité européen de la protection des données sur l'annonce d'un accord de principe sur un nouveau cadre transatlantique pour la protection des données, 6 avril 2022, en ligne à URL : https://cnil.fr/sites/cnil/files/atoms/files/declaration_01-2022_du_cedpb_sur_lannonce_dun_accord_de_principe_sur_un_nouveau_cadre_transatlantique_pour_la_protection_des_donnees.pdf consulté le 10 février 2023.

CNIL, « Données de santé : la CNIL rappelle à deux organismes de recherche médicale leurs obligations légales », Données de santé, 21 mars 2023, en ligne à URL : <https://www.cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-deux-organismes-de-recherche-medicale-leurs-obligations-legales> consulté le 26 juillet 2023.

CNIL, Transfert de données vers les États-Unis : le CEPD rend son avis sur le projet de décision d'adéquation de la Commission européenne, 21 mars 2023, en ligne à URL : <https://www.cnil.fr/fr/transfert-de-donnees-vers-les-etats-unis-le-cepd-rend-son-avis-sur-le-projet-de-decision-dadequation>, consulté le 8 mai 2024.

CNIL, « Transfert de données vers les États-Unis : le CEPD rend son avis sur le projet de décision d'adéquation de la Commission européenne », 23 mars 2023, en ligne à URL : <https://www.cnil.fr/fr/transfert-de-donnees-vers-les-etats-unis-le-cepd-rend-son-avis-sur-le-projet-de-decision-dadequation> consulté le 30 juin 2023

CNIL, « Big data », définition, en ligne à URL : <https://www.cnil.fr/fr/definition/big-data> consulté en ligne le 5 février 2022.

CNIL, « Définition données personnelles », en ligne à URL : <https://www.cnil.fr/fr/definition/donnee-personnelle> consulté en ligne le 3 avril 2023.

CNIL, « Les données sensibles c'est quoi ? », 2023, en ligne à URL : <https://www.cnil.fr/fr/cnil-direct/question/une-donnee-sensible-cest-quoi> consulté le 27 mars 2023.

CNIL, « Le système API-PNR : la vie privée des voyageurs est-elle respectée ? », Question, en ligne à URL : <https://www.cnil.fr/fr/cnil-direct/question/le-systeme-api-pnr-la-vie-privee-des-voyageurs-est-elle-respectee?visiteur=part> consulté le 5 août 2023.

C. COCHARD, « Les aéroports, ces cités des nuages », *Le Temps*, 10 juin 2023, en ligne à URL : <https://www.letemps.ch/societe/aeroports-cites-nuages> consulté le 30 août 2023.

Commission européenne, « Certificat COVID numérique de l'UE », Union européenne, *Communication*, 31 janvier 2022, en ligne à URL : https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_fr consulté le 2 août 2023.

Commission européenne, « Santé dans l'UE : l'espace européen des données de santé (EHDS) », Coin presse, 3 mai 2022, en ligne à URL : https://ec.europa.eu/commission/presscorner/detail/fr/qanda_22_2712 consulté le 25 juillet 2023.

Commission européenne, « Discours de la Présidente von der Leyen sur les relations UE - Chine à l'intention du Mercator Institute for China Studies et du Centre de politique européenne », Discours, 30 mars 2023, en ligne à URL : https://france.representation.ec.europa.eu/informations/discours-de-la-presidente-von-der-leyen-sur-les-relations-ue-chine-lintention-du-mercator-institute-2023-03-30_fr consulté le 21 août 2023.

Confédération suisse, « Consultation concernant la loi sur les données relatives aux passagers aériens, LDPa », *Office fédéral de la police fedpol*, 2022, en ligne à URL : <https://www.fedpol.admin.ch/fedpol/fr/home/polizei-zusammenarbeit/international/flugpassagierdaten.html> consulté en ligne le 23 mars 2023.

Courrier international, « L'OMS met fin à l'urgence de santé publique planétaire pour le Covid-19 », Covid-19, 5 mai 2023, en ligne à URL : <https://www.courrierinternational.com/article/virus-l-oms-met-fin-a-l-urgence-de-sante-publique-planetaire-pour-le-covid-19> consulté le 24 juillet 2023.

European Commission, « Administrative arrangement between the WHO and the European Commission on technical cooperation related to the global digital health certification network », 11 juillet 2023, en ligne à URL :

https://commission.europa.eu/document/d1fb7b2e-0966-4496-a56a-5ab4a35ab15f_en consulté le 2 août 2023.

Commission européenne, « Protection des données personnelles », 2024, en ligne à URL : https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_fr consulté en ligne le 5 mai 2024.

Conseil constitutionnel, décision n° 2019-781 DC du 16 mai 2019, *Communiqué de presse*, 16 mai 2019.

Conseil européen, « Directive de l'UE relative aux données des dossiers passagers (PNR) », *Europa*, Politique, Action de l'UE face au terrorisme, 31 août 2022, en ligne à URL : <https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/passenger-name-record/#pnr> consulté le 24 août 2023.

Conseil européen, « Les systèmes informatiques pour lutter contre la criminalité et sécuriser les frontières de l'UE », *Europa*, Politiques, 13 mars 2023, en ligne à URL : <https://www.consilium.europa.eu/fr/policies/it-systems-security-justice/> consulté le 29 août 2023.

Conseil de l'Union européenne, « Signature de l'accord UE-Canada sur les données des dossiers passagers (données PNR) », Communiqué de presse, 25 juin 2014, Bruxelles, Presse. Conseil de l'Union européenne, « Accord PNR entre l'UE et le Japon: le Conseil autorise l'ouverture de négociations », Communiqué de presse, 18 février 2020, en ligne à URL : <https://www.consilium.europa.eu/fr/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/> consulté le 21 août 2023.

Conseil de l'Union européenne, « Prévention du terrorisme et de l'extrémisme violent et lutte contre ces phénomènes : le Conseil adopte des conclusions sur l'action extérieure de l'UE », Communiqué de presse, 16 juin 2020, <https://www.consilium.europa.eu/fr/press/press-releases/2020/06/16/preventing-and-counteracting-terrorism-and-violent-extremism-council-adopts-conclusions-on-eu-external-action/>

Consilium Europa, « Directive de l'UE relative aux données des dossiers passagers (PNR) », *Action de l'UE face au terrorisme*, Conseil européen – Conseil de l'Union européenne, 31 août 2022, en ligne à URL : <https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/passenger-name-record/#:~:text=La%20directive%20PNR%20r%C3%A9glemente%20le,des%20poursuites%20en%20la%20mati%C3%A8re>

O. CORTEN, « Vers une « déterritorialisation » de l'interdiction du recours à la force dans les relations internationales ? », *Organization of American States*, 7 juillet 2010, en ligne à URL :

http://www.oas.org/dil/esp/XXXVII_Curso_vers_una_Leonardo_Nemer.pdf consulté le 20 juillet 2023.

Coulisses de Bruxelles, « PNR: un fichier des voyageurs aériens inutile », *Libération*, 21 décembre 2015, en ligne à URL : https://www.liberation.fr/debats/2015/12/21/pnr-un-fichier-des-voyageurs-aeriens-inutile_1812825/ consulté le 9 mars 2023.

A. DEIANA, « Coupe du monde au Qatar : la Cnil conseille aux supporters français d'utiliser des téléphones vierges pour prévenir les risques d'espionnage », *France Info*, 15 novembre 2022, en ligne à URL : https://www.francetvinfo.fr/coupe-du-monde/coupe-du-monde-au-qatar-la-cnil-conseille-aux-supporters-francais-d-utiliser-des-telephones-vierges-pour-prevenir-les-risques-d-espionnage_5478510.html consulté le 31 juillet 2023.

G. DELACROIX, S. LANDRIN, « Coronavirus : en Inde, l'impossible confinement des pauvres », *Le Monde*, le 27 mars 2020, en ligne à URL : https://www.lemonde.fr/international/article/2020/03/27/coronavirus-en-inde-l-impossible-confinement-des-pauvres_6034596_3210.html consulté le 24 juillet 2023.

J.-L. DELMAS, « Aviation : Combien d'avions pourrait-on avoir au maximum dans le ciel avant qu'il ne soit saturé ? », *20 Minutes*, 21 juin 2023, en ligne à URL : <https://www.20minutes.fr/economie/4042146-20230621-aviation-combien-pourrait-avoir-maximum-ciel-avant-sature#:~:text=Selon%20le%20Groupe%20d'action,m%C3%AAme%20%C3%AAtre%20multipli%C3%A9%20par%20deux> consulté le 24 août 2023.

T. DE MONTBRIAL, « Conséquences et leçons d'un virus », *Ifri*, 1^{er} juillet 2020, en ligne à URL : <https://www.ifri.org/fr/publications/editoriaux-de-lifri/consequences-lecons-dun-virus> consulté le 24 juillet 2023.

T. DE MONTBRIAL, « Après le multilatéralisme, les grandes guerres ? », *Ifri*, 3 août 2020, en ligne à URL : <https://www.ifri.org/fr/espace-media/lifri-medias/apres-multilateralisme-grandes-guerres> consulté le 24 juillet 2023.

Department of Homeland Security, "Fact Sheet: US-EU Passenger Name Record Agreement Signed", 28 mai 2004, en ligne à URL : <https://www.dhs.gov/publication/passenger-name-records-agreements> consulté le 12 décembre 2023.

Diète nationale du Japon, 16 pages, en ligne à URL : [https://www.shugiin.go.jp/internet/itdb_english.nsf/html/statics/english/kokkaiannai_f2202.pdf/\\$File/kokkaiannai_f2202.pdf](https://www.shugiin.go.jp/internet/itdb_english.nsf/html/statics/english/kokkaiannai_f2202.pdf/$File/kokkaiannai_f2202.pdf) consulté le 1^{er} septembre 2023.

Digital Security Magazine, « Le système ABC est mis à jour pour accélérer les citoyens à franchir les frontières dans les aéroports », 5 octobre 2012, en ligne à URL :

<https://www.digitalsecuritymagazine.com/fr/2012/10/05/el-sistema-abc-system-se-actualiza-para-agilizar-a-los-ciudadanos-el-cruce-de-fronteras-en-aeropuertos/> consulté le 8 juin 2023.

Direction générale du Trésor, « La protection des données personnelles au Japon », 8 mai 2019, en ligne à URL : <https://www.tresor.economie.gouv.fr/Articles/2019/05/08/la-protection-des-donnees-personnelles-au-japon> consulté en ligne le 25 mars 2023.

C. EBERLE, « RGPD ou l'Europe qui innove, protège, et influence », *Les Echos*, 22 octobre 2018, en ligne à URL : <https://www.lesechos.fr/idees-debats/cercle/opinion-rgpd-ou-leurope-qui-innove-protège-et-influence-142493> consulté le 19 juillet 2023.

F. ECALLE, « Les enjeux de la privatisation des aéroports de Paris », *Les commentaires de l'actualité*, *FIPECO*, 3 septembre 2018, en ligne à URL : <https://www.fipeco.fr/pdf/0.22884500%201535967431.pdf> consulté le 10 août 2023.

EDPS, « Données PNR de l'UE : le CEPD met en garde contre une collecte massive et induite des données des passagers », Communiqué de presse, EDPS/2015/085, septembre 2015, en ligne à URL : https://www.edps.europa.eu/sites/default/files/edpsweb_press_releases/edps-2015-08-edps_pnr_fr.pdf consulté le 9 avril 2019.

Europa, « Transfert des données des passagers aériens : pour ou contre ? », *Actualité Parlement européen*, 2012, en ligne à URL : <https://www.europarl.europa.eu/topics/fr/article/20120413STO42885/transfert-des-donnees-des-passagers-aeriens-pour-ou-contre> consulté le 10 juin 2023.

Europa, « Accord entre l'Union européenne et les États-Unis concernant les données des dossiers des passagers aériens », *Eux-Lex*, 26 août 2021, en ligne à URL : <https://eur-lex.europa.eu/FR/legal-content/summary/eu-us-agreement-on-airline-passenger-name-record-data.html#:~:text=les%20personnes%20auront%20le%20droit,quinze%20ans%20pour%20le%20terrorisme> consulté le 10 juillet 2023.

Europe 1, « Vol vers les USA : vos données voyagent aussi », 19 avril 2012, en ligne à URL : <https://www.europe1.fr/international/Vol-vers-les-USA-vos-donnees-voyagent-aussi-362914> consulté le 7 avril 2020.

Europe 1, « Fraude fiscale : le gouvernement cible les 'ultra-riches' et les multinationales », 10 mai 2023, en ligne à URL : <https://www.europe1.fr/economie/le-gouvernement-souhaite-augmenter-de-25-les-controles-fiscaux-des-plus-gros-patrimoines-4182063> consulté le 4 août 2023.

EUSS, le Maghreb et l'Union européenne : vers un partenariat privilégié ? Seminar report, 25 octobre 2014, en ligne à URL :

<https://www.iss.europa.eu/sites/default/files/EUISSFiles/rep04-11.pdf> consulté le 20 janvier 2023.

B. FERRAN, « Prism : Apple, Microsoft et Facebook se confessent timidement » [archive], *Le Figaro*, 17 juin 2013, en ligne à URL : <https://www.lefigaro.fr/secteur/high-tech/2013/06/17/32001-20130617ARTFIG00582-prism-apple-microsoft-et-facebook-se-confessent-timidement.php> consulté le 6 juillet 2023.

R. FLÉCHAUX, « L'observabilité pour assurer la fluidité du trafic à l'aéroport de Rome », *Le Monde Informatique*, 28 août 2023, en ligne à URL : <https://www.lemondeinformatique.fr/actualites/lireamp-l-observabilite-pour-assurer-la-fluidite-du-traffic-a-l-aeroport-de-rome-91369.html> consulté le 29 août 2023.

M. FLORIO, S. GAMBA, C. PANCOTTI, « Panorama des investissements publics et privés de long terme dans la mise au point de vaccins contre la Covid-19 », *Parlement européen*, Département thématique des politiques économiques, scientifiques et de la qualité de la vie, Etudes, mars 2023, en ligne à URL : [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740072/IPOL_STU\(2023\)740072\(SUM01\)_FR.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740072/IPOL_STU(2023)740072(SUM01)_FR.pdf) consulté le 24 juillet 2023.

M. FODÉRE, « Le gouvernement veut interroger les compagnies aériennes pour traquer les fraudeurs fiscaux », *Europe 1*, 10 mai 2023, en ligne à URL : <https://www.europe1.fr/economie/le-gouvernement-veut-interroger-les-compagnies-aeriennes-pour-traquer-les-fraudeurs-fiscaux-4182388> consulté le 4 août 2023.

Forbidden Stories, « À Propos du Projet Pegasus », en ligne à URL : <https://forbiddenstories.org/fr/a-propos-du-pegasus-project/> consulté le 3 juillet 2023.

France info, « https://www.francetvinfo.fr/monde/chine/hong-kong/hong-kong-enregistre-une-baisse-record-de-sa-population-apres-une-emigration-massive-des-residents_5305204.html », *France info avec AFP*, 12 août 2022, en ligne à URL : https://www.francetvinfo.fr/monde/chine/hong-kong/hong-kong-enregistre-une-baisse-record-de-sa-population-apres-une-emigration-massive-des-residents_5305204.html consulté le 24 juillet 2023.

France 24, « Aéroports de Paris : pas de référendum, mais un report de la privatisation », 12 mars 2020, en ligne à URL : <https://www.france24.com/fr/20200312-a%C3%A9roports-de-paris-pas-de-r%C3%A9f%C3%A9rendum-mais-un-report-de-la-privatisation> consulté le 22 avril 2023.

France 24, « 11-Septembre : de Manhattan à Brooklyn, mémoires d'une journée en enfer », 9 septembre 2021, en ligne à URL :

<https://www.france24.com/fr/am%C3%A9riques/20210909-11-septembre-de-manhattan-%C3%A0-brooklyn-m%C3%A9moires-d-une-journ%C3%A9e-en-enfer> consulté le 19 septembre 2023.

B. GELLMAN, L. POITRAS, « U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program », *The Washington Post*, 6 juin 2013, en ligne à URL : https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1 consulté le 6 juillet 2023.

F. GLAIN, « Les immigrants acadiens au XVIII^e siècle, une colonie en Poitou », Centre Châtelleraudais d'Histoire et d'Archives, 2018, en ligne à URL : <http://ccha.fr/wp-content/uploads/2018/02/6-Acadiens-PDF.pdf> consulté le 12 juin 2023.

Gouvernement français, « Adoption du PNR par le Parlement européen », *Communiqué*, 14 avril 2016, en ligne à URL : <https://www.gouvernement.fr/partage/6939-adoption-du-pnr-par-le-parlement-europeen> consulté le 24 août 2023.

Gouvernement français, « Adoption du PNR européen : une étape indispensable dans le renforcement de la lutte contre le terrorisme », *Argumentaire*, 15 avril 2016, en ligne à URL : <https://www.gouvernement.fr/argumentaire/adoption-du-pnr-europeen-une-etape-indispensable-dans-le-renforcement-de-la-lutte-4405> consulté le 15 juin 2023.

Gouvernement français, Définition, « Transport public ou privé », *Ministère de la Transition écologique et de la Cohésion des territoires – Ministère de la Transition énergétique*, en ligne à URL : <https://www.ecologie.gouv.fr/transport-public-ou-prive> consulté le 11 janvier 2023.

G. GREENWALD, « NSA Prism program taps in to user data of Apple, Google and others », *The Guardian*, 7 juin 2013, en ligne à URL : <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> consulté le 5 avril 2020.

Groupe ADP, « Politique Groupe de Protection des Données à caractère personnel », 12 novembre 2020, en ligne à URL : <https://www.parisaeroport.fr/docs/default-source/groupe-fichiers/rse/group-personal-data-protection-policy---french-version-only.pdf> consulté le 11 mai 2023.

R. GUBERT, B. ESCHAPASSE, « DGSE : « Nous avons la clandestinité en héritage », *Le Point*, International, Entretien avec le patron de la DGSE Bernard Émié, 28 juin 2023, en ligne à URL : https://www.lepoint.fr/monde/dgse-nous-avons-la-clandestinite-en-heritage-28-06-2023-2526465_24.php#11 consulté le 21 août 2023.

A. GUILLEMOLES, « Covid-19 : les pays pauvres attendent toujours les vaccins Covax », *La Croix*, 2 juillet 2021, en ligne à URL : <https://www.la-croix.com/Economie/Covid-19-pays-pauvres-attendent-toujours-vaccins-Covax-2021-07-02-1201164379> consulté le 24 juillet 2023.

Gulf Times, « No Covid negative certificate needed for travellers from China », Qatar, 28 mars 2023, en ligne à URL : <https://www.gulf-times.com/article/658394/qatar/no-covid-negative-certificate-needed-for-travellers-from-china> consulté le 31 juillet 2023.

G. HAAS, « Directive PNR : la CJUE recadre le traitement des données de passagers aériens », *HAAS Avocats*, le Blog, 16 août 2022, en ligne à URL : <https://info.haas-avocats.com/droit-digital/directive-pnr-la-cjue-recadre-le-traitement-des-donnees-de-passagers-aeriens#:~:text=La%20directive%20PNR%20vise%20%C3%A0,de%20donn%C3%A9es%20de%20personnes%20recherch%C3%A9es>. consulté le 30 juin 2023.

C. HALPERN, D. LORRAIN, « HUB (aéroports et ports) », *Flux*, n° 79-80, pp. 140-152, 2010 ; en ligne sur : <https://www.cairn.info/revue-flux1-2010-1-page-140.htm?contenu=article>

T. HAMMARBERG, Commissaire aux droits de l'homme du Conseil de l'Europe, « Le profilage racial et religieux n'a pas sa place dans la lutte anti-terroriste », 29 mai 2007 ; en ligne sur : http://www.coe.int/t/commissioner/Viewpoints/070529_fr.asp

M. HENRY, « Après le scandale des écoutes, NSO, le fabricant du logiciel espion Pegasus, fait un grand ménage », *Le Figaro*, 21 août 2022, en ligne à URL : <https://www.lefigaro.fr/secteur/high-tech/depart-du-pdg-de-nso-fabricant-du-controverse-logiciel-espion-pegasus-20220821> consulté le 3 juillet 2023.

Human Rights Watch, « Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act », 14 septembre 2017, en ligne à URL : <https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance> consulté le 22 août 2023.

ICO, Penalty notice, COM0783542, British Airways pie, en ligne à URL : <https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf> consulté le 20 juillet 2023.

Intelligence Online, « Les cartels mexicains à la rescousse (involontaire) de la prolongation de l'article 702 sur les interceptions », États-Unis, 27 avril 2023, en ligne à URL : <https://www.intelligenceonline.fr/renseignement-d-etat/2023/04/27/les-cartels-mexicains-a-la->

rescousse-involontaire-de-la-prolongation-de-l-article-702-sur-les-interceptions,109948918-art consulté le 22 août 2023.

O. JAMES, « L'aéroport de Roissy déploie un arsenal antidrones », *Hologarde*, 8 juin 2019 ; en ligne sur : <https://hologarde.com/wp-content/uploads/2019/06/UsineNouvelle-Hologarde.pdf>

S. KEHAULANI GOO, "Northwest Gave U.S. Data on Passengers", *Washington Post*, 18 janvier 2004, en ligne à URL : <https://www.washingtonpost.com/archive/politics/2004/01/18/northwest-gave-us-data-on-passengers/9d1ff042-47a8-41e8-bb5a-ec5535a80841/> consulté le 2 avril 2023.

S. KEHAULANI GOO, "U.S. to Push Airlines for Passenger Records", *Washington Post*, 12 janvier 2004, en ligne à URL : <https://www.washingtonpost.com/archive/politics/2004/01/12/us-to-push-airlines-for-passenger-records/16e2a7e9-c14f-4cd6-8a62-82065de24480/> consulté le 25 mars 2021.

S. KEHAULANI GOO, "American Airlines Revealed Passenger Data", *Washington Post*, 10 avril 2004, en ligne à URL : <https://www.washingtonpost.com/archive/business/2004/04/10/american-airlines-revealed-passenger-data/e0584179-eea7-4f0a-9c0d-07b7e1a83f89/> consulté le 2 avril 2023.

M. KERSHNER, "Data isn't the new oil – Time is", *Forbes*, 15 juillet 2021, en ligne à URL : <https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/> consulté le 27 août 2023.

J. KREWER, « La donnée est-elle le nouveau pétrole ou un nouvel environnement ? », *Usbek & Rica*, 9 mai 2018, en ligne à URL : <https://usbeketrica.com/fr/article/quatre-metaphores-pour-une-politique-de-la-donne> consulté le 28 août 2023.

J. LAGASSE, « "Fichier" PNR : surveillance électronique de masse ou nouveau paradigme de la sécurité ? », *Les Notes du CREOGN*, n° 19, 2016 ; en ligne sur : <https://hal.science/hal-03096592/document>

D. LE DOUSSAL, S. HATANO, « Réforme de la loi sur la protection des informations personnelles au Japon », *CCI France Japon*, Analyses & Études, 17 mai 2017, en ligne à URL : <https://www.ccifj.or.jp/publications/actus/n/news/reforme-de-la-loi-sur-la-protection-des-informations-personnelles-au-japon.html> consulté en ligne le 25 mars 2023.

Légifrance, « Observations du Gouvernement sur la loi relative au renseignement », *Journal officiel électronique authentifié*, 26 juillet 2015, en ligne à URL : <https://www.legifrance.gouv.fr/jorf/id/JORFARTI000030932377#JORFARTI000030932377> consulté le 5 août 2023.

D. LELOUP, M. UNTERSINGER, « 'Projet Pegasus' : révélations sur un système mondial d'espionnage de téléphones », *Le Monde*, 4 novembre 2022, en ligne à URL : https://www.lemonde.fr/projet-pegasus/article/2021/07/18/projet-pegasus-revelations-sur-un-systeme-mondial-d-espionnage-de-telephones_6088652_6088648.html?random=1430103654 consulté le 3 juillet 2023.

L'Express, « Attentats: qu'est-ce que le PNR, ce fichier européen qui fait tant polémique ? », 23 mars 2016, en ligne à URL : https://www.lexpress.fr/monde/europe/attentats-qu-est-ce-que-le-pnr-ce-fichier-europeen-qui-fait-tant-polemique_1775994.html consulté le 20 mars 2024.

Le Figaro, « Attentats de Paris : le point sur l'enquête 24 heures après les faits », 13 novembre 2015, en ligne à URL : <https://www.lefigaro.fr/actualite-france/2015/11/14/01016-20151114ARTFIG00228-attentats-de-paris-le-point-sur-l-enquete-24-heures-apres-les-faits.php> consulté le 19 septembre 2023.

Le Figaro, « Covid-19 : le gouvernement britannique renonce au passeport vaccinal », *Le Figaro avec AFP*, 12 septembre 2021, en ligne à URL : <https://www.lefigaro.fr/international/covid-19-le-gouvernement-britannique-renonce-au-passeport-vaccinal-20210912> consulté le 2 août 2023.

Le Figaro, « Hongrie : cinquième jour de manifestations contre une réforme d'Orban », 17 juillet 2022, en ligne à URL : <https://www.lefigaro.fr/flash-eco/hongrie-cinquieme-jour-de-manifestations-contre-une-reforme-d-orban-20220717> consulté le 17 août 2023.

Le Figaro, « L'Union européenne adopte un nouveau cadre légal pour le transfert de données vers les États-Unis », *Tech & web*, 10 juillet 2023, en ligne à URL : <https://www.lefigaro.fr/secteur/high-tech/l-union-europeenne-adopte-un-nouveau-cadre-legal-pour-le-transfert-de-donnees-vers-les-etats-unis-20230710> consulté le 22 août 2023.

D. LELOUP ET M. SZADKOWSKI, « Prism, Snowden, surveillance : 7 questions pour tout comprendre », *Le Monde*, 2 juillet 2013, en ligne à URL : https://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html consulté le 19 août 2022.

Le Monde.fr avec AFP et Reuters, « Prism : la NSA espionnait l'Union européenne », *Le Monde*, 29 juin 2013, en ligne à URL : https://www.lemonde.fr/ameriques/article/2013/06/29/prism-la-nsa-espionnait-l-union-europeenne_3439112_3222.html consulté le 6 juillet 2023.

Le Monde, « L'Italie rejoint les « nouvelles routes de la soie » de la Chine », 23 mars 2019, en ligne à URL : <https://www.lemonde.fr/economie/article/2019/03/23/malgre-l-inquietude->

[de-bruxelles-l-italie-rejoint-les-nouvelles-routes-de-la-soie-de-pekine_5440367_3234.html](https://www.lemonde.fr/bruxelles-l-italie-rejoint-les-nouvelles-routes-de-la-soie-de-pekine/article/2020/03/14/italie-rejoint-les-nouvelles-routes-de-la-soie-de-pekine_5440367_3234.html)

consulté le 30 août 2024.

Le Monde, « Coronavirus : Édouard Philippe annonce la fermeture de tous les lieux publics ‘non indispensables’ », Politique, Coronavirus et Pandémie de Covid-19, 14 mars 2020, en ligne à URL : https://www.lemonde.fr/politique/article/2020/03/14/edouard-philippe-annonce-la-fermeture-de-tous-les-lieux-publics-non-indispensables_6033110_823448.html

consulté le 24 juillet 2023.

Le Monde, « British Airways et Marriott écotent de lourdes amendes pour des données personnelles mal sécurisées », Pixels, Vie privée, 2 novembre 2020, en ligne à URL : https://www.lemonde.fr/pixels/article/2020/11/02/british-airways-et-marriott-ecotent-de-lourdes-amendes-pour-des-donnees-personnelles-mal-securisees_6058212_4408996.html

consulté le 20 juillet 2023.

Le Monde, « Pauvreté et crise du multilatéralisme, comment le Covid-19 aggrave les fractures mondiales », Débats, Coronavirus et pandémie de Covid-19, 9 avril 2021, en ligne à URL : https://www.lemonde.fr/idees/article/2021/04/09/pauvrete-et-crise-du-multilateralisme-comment-le-covid-19-aggrave-les-fractures-mondiales_6076110_3232.html

consulté le 24 juillet 2023.

Le Monde, « Passe sanitaire : débats électriques à l’Assemblée nationale », *Le Monde avec AFP*, 22 juillet 2021, en ligne à URL : https://www.lemonde.fr/politique/article/2021/07/22/passe-sanitaire-les-deputes-prolongent-les-debats_6089126_823448.html

Le Monde, « L’ONU estime que 274 millions de personnes dans le monde auront besoin d’une aide d’urgence en 2022 », Planète, Sécuritaire alimentaire, 2 décembre 2021, en ligne à URL : https://www.lemonde.fr/planete/article/2021/12/02/l-onu-estime-que-274-millions-de-personnes-dans-le-monde-aurent-besoin-d-une-aide-d-urgence-en-2022_6104411_3244.html

Le Monde, « États-Unis : le chef d’extrême droite Stewart Rhodes condamné à dix-huit ans de prison pour "sédition" » lors de l’assaut du Capitole », 25 mai 2023, en ligne à URL : https://www.lemonde.fr/international/article/2023/05/25/etats-unis-le-chef-d-extreme-droite-stewart-rhodes-condamne-a-dix-huit-ans-de-prison-pour-sedition-lors-de-l-assaut-du-capitole_6174865_3210.html

Le Monde, « Max Schrems : ‘Le RGPD a une influence parce qu’il est et continuera d’être le standard mondial’ », 25 mai 2023, en ligne à URL : [https://www.lemonde.fr/pixels/article/2023/05/25/max-schrems-le-rgpd-a-une-influence-](https://www.lemonde.fr/pixels/article/2023/05/25/max-schrems-le-rgpd-a-une-influence-standard-mondial_6174865_3210.html)

[parce-qu'il-est-et-continuera-a-etre-le-standard-mondial 6174747 4408996.html](#) consulté le 19 juillet 2023.

J. LIBOREIRO, « Les six principaux points de friction entre l'UE et la Chine », *Euronews*, 3 avril 2023, en ligne à URL : [https://fr.euronews.com/my-europe/2023/04/03/les-six-principaux-points-de-friction-entre-lue-et-la-chine](#) consulté le 21 août 2023 .

L. LICTEVOUT, B. GAILLARD, « La politique numérique de l'Union européenne », *Toute l'Europe*, 27 mars 2023, en ligne à URL : [https://www.touteleurope.eu/economie-et-social/la-politique-numerique-de-l-union-europeenne/](#) consulté en ligne le 14 juin 2023.

Ligue des droits de l'Homme, *Protection des données personnelles*, Analyse comparée des législations et des pratiques dans neuf pays européens dans le contexte du cadre juridique européen, juin 2010, en ligne à URL : [https://www.ldh-france.org/wp-content/uploads/IMG/pdf/SynthesfrancaisFINALcorr-BD.pdf](#) consulté le 29 août 2023.

Ligue des droits de l'Homme, « Nouvel accord PNR (UE-USA) : Pas d'amélioration, le PE doit le rejeter ! », données personnelles, 25 janvier 2012, en ligne à URL : [https://www.ldh-france.org/Nouvel-accord-PNR-UE-USA-pas-d/](#) consulté le 21 août 2023.

Ligue des droits humains, « La loi belge PNR 'Passenger Name Record' recadrée par la Cour de justice de l'Union européenne », Communiqué de presse, 21 juin 2022, en ligne à URL : [https://www.liguedh.be/la-loi-belge-pnr-passenger-name-record-recadree-par-la-cour-de-justice-de-lunion-europeenne/](#) consulté en ligne le 31 mars 2023.

E. LIPTON, "U.S. Official Admits to Big Delay in Revamping No-Fly Program", *New York Times*, 21 février 2007, en ligne à URL : [https://www.nytimes.com/2007/02/21/washington/21secure.html](#) consulté le 22 mars 2022.

E. MACASKIL, « NSA paid millions to cover Prism compliance costs for tech companies », *The Guardian*, 23 août 2013, en ligne à URL : [https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid](#) consulté le 12 avril 2023.

E. MACRON, « La France unie, c'est notre meilleur atout dans la période troublée par le Covid-19 que nous traversons. Nous tiendrons. Tous ensemble », Adresse aux Français, *Élysée*, 12 mars 2020, en ligne à URL : [https://www.elysee.fr/emmanuel-macron/2020/03/12/adresse-aux-francais](#) consulté le 23 juillet 2023.

Maroc.ma, « M. Jouahri : La protection des données revêt une importance capitale pour Bank Al Maghrib », Actualité, 14 juin 2019, en ligne à URL : [https://aujourd'hui.ma/economie/la-protection-des-donnees-revet-une-importance-capitale-pour-bank-al-maghrib](#) consulté le 15 février 2020.

S. E. MARTONONSI, A. BARNETT, “How Effective Is Security Screening Of Airline Passengers?”, *Interfaces*, 36(6), 2006, pp. 545–552, en ligne à URL : https://www.researchgate.net/publication/220249989_How_Effective_Is_Security_Screening_of_Airline_Passengers consulté le 10 janvier 2020.

F. MASELLI, « Le casse-tête chinois de Meloni : enquête au cœur de l’Italie des Nouvelles Routes de la soie », *Le Grand Continent*, 9 juillet 2023, en ligne à URL : <https://legrandcontinent.eu/fr/2023/07/09/le-casse-tete-chinois-de-meloni-enquete-au-coeur-de-litalie-des-nouvelles-routes-de-la-soie/> consulté le 21 août 2023.

G. MAUJEAN, « Comment un faux tweet a fait plonger Wall Street », *Les Échos*, 24 avril 2013, en ligne à URL : <https://www.lesechos.fr/2013/04/comment-un-faux-tweet-a-fait-plonger-wall-street-338456> consulté en ligne le 15 février 2022.

C. MESTRE, S. MINASSIAN, M. R. MORO, « Ondes de choc après l’assassinat de Samuel Paty », *L’autre*, 2021, pp. 4-6, en ligne à URL : <https://www.cairn.info/revue-l-autre-2021-1-page-4.htm> consulté le 20 septembre 2023.

Ministère de l’Économie, des finances et de la souveraineté industrielle et numérique, « Pass vaccinal : toutes les informations », 8 mars 2022, en ligne à URL : <https://www.economie.gouv.fr/pass-vaccinal-informations#> consulté le 2 août 2023.

Ministère de l’Intérieur et des outre-mer, « Covid-19 : déplacements internationaux », 1^{er} août 2022, en ligne à URL : <https://www.interieur.gouv.fr/covid-19/deplacements-internationaux> consulté le 31 juillet 2023.

Ministère de l’Intérieur, « En 2025, l’Union européenne déploie de nouveaux outils dédiés aux voyageurs étrangers pour sécuriser son territoire », 19 septembre 2023, en ligne à URL : <https://www.interieur.gouv.fr/actualites/actualites-du-ministere/en-2025-lunion-europeenne-deploie-de-nouveaux-outils-dedies-aux> consulté le 19 novembre 2023.

P. MUNTEAN, D. COLE, “25-year anniversary of TWA Flight 800 explosion marks new chapter in disaster's history”, *CNN*, 18 juillet 2021, en ligne à URL : <https://edition.cnn.com/2021/07/17/politics/twa-flight-800-wreckage-destroyed-memorial/index.html> consulté le 27 avril 2023.

MyHealth@EU est une infrastructure numérique transfrontalière permettant d’échanger des données de santé recueillies lors de prestations de soins. En ligne à URL : https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_fr consulté le 25 juillet 2023.

V. NEIRINCK-FAUVELLE, « Données personnelles : le régulateur irlandais inflige une amende record de 1,2 milliard d’euros à Meta », *Toute l’Europe*, Numérique droits

fondamentaux, Revue de presse, 23 mai 2023, en ligne à URL : <https://www.touteleurope.eu/l-ue-dans-le-monde/donnees-personnelles-le-regulateur-irlandais-inflige-une-amende-record-de-12-milliard-d-euros-a-meta/> consulté le 22 août 2023.

S. OMARJEE, J. BELOT, « L'accès au PNR pour lutter contre la fraude fiscale : une nouvelle menace pour la vie privée ? », *Village de la justice*, en ligne à URL : [https://www.village-justice.com/articles/acces-pnr-pour-lutter-contre-fraude-fiscale-une-nouvelle-menace-pour-vie-privée,46364.html#:~:text=L'annonce%20du%20ministre%20des,PNR%20\(Passengers%20N%20Record\)](https://www.village-justice.com/articles/acces-pnr-pour-lutter-contre-fraude-fiscale-une-nouvelle-menace-pour-vie-privée,46364.html#:~:text=L'annonce%20du%20ministre%20des,PNR%20(Passengers%20N%20Record)) consulté le 4 août 2023.

OMS, « Stratégie Covid-19 », 14 avril 2020, en ligne à URL : https://www.who.int/docs/default-source/coronaviruse/strategy-update-french.pdf?sfvrsn=b1cfe48a_2 consulté le 24 juillet 2023.

OMS, « L'Assemblée mondiale de la Santé convient d'entamer un processus visant à élaborer un accord mondial historique sur la prévention, la préparation et la riposte face aux pandémies », Communiqué de presse, 1^{er} décembre 2021, en ligne à URL : <https://www.who.int/fr/news/item/01-12-2021-world-health-assembly-agrees-to-launch-process-to-develop-historic-global-agreement-on-pandemic-prevention-preparedness-and-response> consulté le 24 juillet 2023.

OMS, « Accord mondial sur la prévention, la préparation et la riposte face aux pandémies », Q&R, 28 juin 2023, en ligne à URL : <https://www.who.int/fr/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/pandemic-prevention--preparedness-and-response-agreement> consulté le 24 juillet 2023.

Organisation de l'aviation civile internationale, « Le rôle du voyage fluide et sans contact dans la relance du transport aérien au cœur de l'édition 2021 du Symposium TRIP », Communiqué, Montréal, 26 mai 2021, en ligne à URL : <https://www.icao.int/Newsroom/NewsDoc2021fix/COM.36.21.FR.pdf> 29 août 2023.

Orly Facile, « Formalités voyages », *Aéroport Orly*, 2023, en ligne à URL : <https://www.orly-aeroport.fr/formalites-voyage/> consulté le 12 mai 2023.

M. PALMER, "Data is the new oil!", ANA Marketing Maestros, 2006, en ligne à URL: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html consulté le 27 août 2023.

Parlement européen, « Le Parlement approuve le renforcement des pouvoirs d'Europol, mais pas sans contrôle », Communiqué de presse, 4 mai 2022.

Parlement européen, « Émissions de CO2 des avions et des navires : faits et chiffres (infographie) », Société, 14 juin 2022, en ligne à URL :

<https://www.europarl.europa.eu/news/fr/headlines/society/20191129STO67756/emissions-de-co2-des-avions-et-des-navires-faits-et-chiffres-infographie> consulté le 28 août 2023.

Parlement européen, « Les institutions européennes approuvent la déclaration sur les droits et principes numériques », Communiqué de presse, 15 décembre 2022.

J. PAVAUX, « Quel est le vrai bilan socio-économique des aéroports français ? », *Jacques Pavaux Conseil*, 30 novembre 2021, en ligne à URL : https://www.fnaut.fr/uploads/2022/05/Jacques_Pavaux_Se%CC%81nat_Impact_e%CC%81conomique_ae%CC%81roportVF3.pdf consulté le 12 avril 2022.

B. PEDROLETTI, « En Chine, le « crédit social » des citoyens fait passer les devoirs avant les droits », *Le Monde*, 16 janvier 2020 en ligne à URL : https://www.lemonde.fr/idees/article/2020/01/16/le-credit-social-les-devoirs-avant-les-droits_6026047_3232.html consulté le 27 juin 2023.

A. PETEL, « Le rôle du parlement européen dans la protection des données personnelles », *Les Surligneurs*, 24 mai 2019, en ligne à URL : <https://www.lessurligneurs.eu/le-role-du-parlement-europeen-dans-la-protection-des-donnees-personnelles/> consulté en ligne le 29 mars 2023.

S. PEYROU, « De l'accord PNR à Prism, bilan et perspectives sur les malentendus transatlantiques : lutte anti-terroriste versus protection des données personnelles », *GDR-ELSJ*, 11 septembre 2013, en ligne à URL : <https://www.gdr-elsj.eu/2013/09/11/droits-fondamentaux/de-laccord-pnr-a-prism-bilan-et-perspectives-sur-les-malentendus-transatlantiques-lutte-anti-terroriste-versus-protection-des-donnees-personnelles/> consulté le 9 mai 2022.

D. PHILLIPS, “JetBlue Apologizes for Use of Passenger Records”, *Washington Post*, 20 septembre 2003, en ligne à URL : <https://www.washingtonpost.com/archive/business/2003/09/20/jetblue-apologizes-for-use-of-passenger-records/207e5529-db29-40f3-9e27-6195faed2bff/> consulté le 8 juin 2020.

A. PIQUARD, « Europe - États-Unis : l'accord transatlantique controversé de transfert des données validé par Bruxelles », *Le Monde*, 10 juillet 2023, en ligne à URL : https://www.lemonde.fr/economie/article/2023/07/10/europe-etats-unis-laccord-transatlantique-controverse-de-transfert-des-donnees-valide-par-bruxelles_6181378_3234.html consulté le 22 août 2023.

F. POCHÉ, « Diagnostiquer le mécontentement », *Revue Projet*, 29 janvier 2020, en ligne à URL : <https://www.revue-projet.com/articles/2020-01-poche-diagnostiquer-le-mecontentement/10464> consulté le 12 juin 2023.

M. PONTRUCHER, « Accord entre l'Union européenne et les États-Unis sur le transfert de données : jamais deux sans trois ? », *Digitemis*, 22 octobre 2022, en ligne à URL : <https://www.digitemis.com/accord-union-europeenne-etats-unis-transfert-de-donnees/> consulté le 20 septembre 2023.

A. PRIESTLEY, M. BEAUVAIS, "International experience and good practices in API/PNR", *OSCE*, 2021, en ligne à URL : <https://www.osce.org/files/f/documents/a/a/510575.pdf> consulté le 4 août 2023.

Privacy Solved, "Data Protection Is Trending In The Middle East", Briefing, en ligne à URL: <https://www.privacysolved.com/data-protection-is-trending-in-the-middle-east/> consulté en ligne le 6 mars 2023.

C. PUDLOWSKI, « David Thomson : "L'Europe est condamnée à subir le contre-choc des erreurs qui ont été faites" », *Slate*, 20 décembre 2016, en ligne à URL : <https://www.slate.fr/story/131831/erreurs-medias-djihadisme> consulté le 17 mai 2023.

Qatar Airways, "Qatar Airways Partner Agency Policies", *Airline Policy (COM-100)*, 31 mars 2021, en ligne à URL : https://www.qatarairways.com/content/dam/tradepartners/pdf-files/QAPAP_Qatar-Airways-Partner-Agency-Policies.pdf consulté en ligne le 23 mars 2023.

I. RAVID. "Safety Versus Defense: Comments on "CAPPS II: The Foundation of Aviation Security?", *Risk Analysis*, 2004. GAO, Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385, 2004, en ligne à URL : <https://onlinelibrary.wiley.com/doi/10.1111/j.0272-4332.2004.00493.x> consulté le 2 avril 2023.

G. REILHAC, « Feu vert du Parlement européen à la collecte des données PNR », *Reuters*, Sociétés, 14 avril 2016, en ligne à URL : <https://www.reuters.com/article/union-parlement-pnr-idFRL5N17H2Q0> consulté le 10 août 2023.

A. REVERCHON, « Robert Boyer : 'Le capitalisme sort considérablement renforcé par cette pandémie' », *Economie française*, *Le Monde*, 2 octobre 2020, en ligne à URL : https://www.lemonde.fr/idees/article/2020/10/02/robert-boyer-le-capitalisme-sort-considerablement-renforce-par-cette-pandemie_6054441_3232.html consulté le 21 juillet 2023.

R. RIVAIS, « Le transfert de données passagers aux États-Unis jugé illégal », *Le Monde*, le 30 mai 2006, en ligne à URL : https://www.lemonde.fr/europe/article/2006/05/30/le-transfert-de-donnees-passagers-aux-etats-unis-juge-illegal_777609_3214.html consulté le 20 mars 2023.

F. RIVIERE, « Bernard Squarcini: ‘Il faut renforcer les moyens des services de renseignement’ », *RFI*, 13 février 2015, en ligne à URL : <https://www.rfi.fr/fr/emission/20150213-bernard-squarcini-invite-frederic-riviere-services-renseignements-terrorisme> consulté le 24 août 2023.

D. ROUCAUTE, « Covid-19, maladies non transmissibles, pollution : l’OMS dresse son bilan de la santé mondiale », *Le Monde*, 19 mai 2023, en ligne à URL : https://www.lemonde.fr/planete/article/2023/05/19/covid-19-maladies-non-transmissibles-pollution-l-oms-dresse-son-bilan-de-la-sante-mondiale_6173967_3244.html consulté le 31 juillet 2023.

J.-J. SARFATI, « Des limites de l’idée du droit flexible », *Le Philosophoire*, 2012/2, n°38, pp. 207 à 228, 2012, en ligne à URL : <https://www.cairn.info/revue-le-philosophoire-2012-2-page-207.htm> consulté le 24 août 2023.

R. SCHUMAN, *Discours de l’horloge*, 9 mai 1950, en ligne à URL : <https://www.strasbourg-europe.eu/la-declaration-schuman/> consulté le 10 juillet 2022.

V. K. SENGUPTA, « Geneva Conventions are outdated, say US envoy », *Independent* (London), 22 février 2022, p. 1, en ligne à URL : <https://www.independent.co.uk/news/world/americas/geneva-conventions-are-outdated-says-us-envoy-9194166.html> consulté le 27 mars 2023.

P. SLEVIN, G. LARDNER JR., « Bush Plan for Terrorism Trials Defended », *Washington Post*, 15 novembre 2001, en ligne à URL : <https://www.washingtonpost.com/archive/politics/2001/11/30/bush-defends-secret-tribunals-for-terrorism-suspects/3714c537-50fb-49e6-87b6-2d386259368d/> consulté le 12 avril 2023.

A. SYLLA, « Recent developments in African data protection laws - Outlook for 2023 », *Hogan Lovells*, février 2023, en ligne à URL : <https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45> consulté en ligne le 8 mars 2023.

N. SWEENY, « Raphaël Kempf : ‘Il y a une criminalisation de l’action politique’ », *Politis*, 11 janvier 2023, en ligne à URL : <https://www.politis.fr/articles/2023/01/il-y-a-une-criminalisation-de-laction-politique-raphael-kempf/> consulté en ligne le 18 février 2022.

S. TAYLOR, “Big brother and another overblown privacy scare”, *The Atlantic*, 2002, en ligne à URL : <https://www.theatlantic.com/politics/archive/2002/12/big-brother-and-another-overblown-privacy-scare/378110/> consulté le 10 mars 2022.

Thales, « La surveillance des frontières, un défi complexe », Surveillance des frontières, en ligne à URL : <https://www.thalesgroup.com/fr/global/activities/security/state/surveillance-des-frontieres> consulté le 8 juin 2023.

Thales, « Thales et Inetum améliorent le passage aux frontières dans les aéroports espagnols de Valence et Bilbao », 25 mars 2021, en ligne à URL : <https://www.thalesgroup.com/fr/group/journaliste/press-release/thales-et-inetum-ameliorent-le-passage-aux-frontieres-aeroports> consulté le 8 juin 2023.

Thales, « Le système électronique d'Entrée-Sortie en zone Schengen: la biométrie au service des frontières intelligentes », en ligne à URL : <https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/biometrie/systeme-entree-sortie> consulté le 15 janvier 2024.

S. TENENBAUM, « Belt And Road Initiative : Quels enjeux pour la Chine et ses partenaires ? », *BSI Economics*, 12 mars 2019, en ligne à URL : <https://www.bsi-economics.org/977-belt-road-initiative-enjeux-chine-partenaires-st> consulté le 21 août 2023.

The Daily Journal of the of the United States Government, Security of Checked Baggage on Flights Within the United States, Federal Register, A Proposed Rule by the Federal Aviation Administration on 04/19/1999, en ligne à URL : <https://www.federalregister.gov/documents/1999/04/19/99-9635/security-of-checked-baggage-on-flights-within-the-united-states> consulté le 20 mars 2023.

Toute l'Europe, « Covid-19 : le pass sanitaire européen a été efficace, selon un nouveau rapport », *Comprendre l'Europe*, 11 janvier 2023, en ligne à URL : <https://www.touteleurope.eu/societe/covid-19-le-pass-sanitaire-europeen-a-ete-efficace-selon-un-nouveau-rapport/> consulté le 2 août 2023.

G. TOPHAM, "Gatwick drone disruption cost airport just £1.4m", *Guardian*, 18 juin 2019, en ligne à URL : <https://www.theguardian.com/uk-news/2019/jun/18/gatwick-drone-disruption-cost-airport-just-14m> consulté le 25 juin 2023.

Transportation Security Administration, "TSA's CAPPS II Gives Equal Weight to Privacy, Security," Press Release, 11 mars 2003, en ligne à URL : https://itlaw.fandom.com/wiki/Transportation_Security_Administration consulté le 9 mars 2020.

F. TRUONG, « Le drame de Conflans-Sainte-Honorine nous rappelle qu'une salle de classe n'est pas une arène politique publique », *Le Monde*, 2020, en ligne à URL : <http://www.lemonde.fr/idees/article/2020/11/23/fabien-truong-le-drame-de-conflans-sainte->

honorine-nous-rappelle-qu-une-salle-de-classe-n-est-pas-une-arene-politique-publique_6060745_3232.html consulté le 20 septembre 2023.

Union européenne, « Le CEPD rend un avis sur le nouvel accord UE-USA sur les données des dossiers passagers (données PNR) », communiqué de presse, le 13 décembre 2011, en ligne à URL : https://www.edps.europa.eu/sites/default/files/edpsweb_press_releases/edps-2011-12_us-pnr_fr.pdf consulté le 12 juin 2023.

U.S. Customs and Border Protection, Passenger Name Record (PNR), 2023, en ligne à URL : <https://www.cbp.gov/travel/clearing-cbp/passenger-name-record> consulté le 27 mars 2023.

U.S. Department of Homeland Security, “DHS Can Strengthen Its International Cybersecurity Programs” OIG-12-112, 2012, pp.12-14, en ligne à URL <https://www.hsdl.org/?view&did=722620> consulté le 23 septembre 2023.

Usito, « Intrusif », Définition, Dictionnaire de l’Université de Sherbrooke, en ligne à URL : <https://usito.usherbrooke.ca/d%C3%A9finitions/intrusif> consulté le 21 juin 2023.

C. VALLET, « Fichés jusqu’au ciel ? », *Alternatives économiques*, 2015, p. 19, en ligne à URL : <https://www.alternatives-economiques.fr/fiches-jusquau-ciel/00073245> consulté le 21 avril 2022.

A. VAN BRUNT, « The ‘torture’ memos prove America’s lawyers don’t know how to be ethical », *The Washington Post*, 12 décembre 2014, en ligne à URL : <https://www.washingtonpost.com/posteverything/wp/2014/12/12/the-torture-memos-prove-americas-lawyers-dont-know-how-to-be-ethical/> consulté le 7 janvier 2020.

B. VAN DER SLOOT, “Passenger Name Record”, European Human Rights Cases, 2017, en ligne à URL : <https://bartvandersloot.com/onewebmedia/pnr.pdf> consulté le 24 août 2023.

M. VEAUDOR, « Politique pénale et préjugé racial aux États-Unis », *La vie des idées*, 6 mars 2016, en ligne à URL : https://laviedesidees.fr/IMG/pdf/20170306_massincarceration.pdf consulté le 3 octobre 2023.

N. VERSIEUX, « Berlin et Bruxelles tirent les grandes oreilles de l’Amérique », *Libération*, 30 juin 2013, en ligne à URL : https://www.liberation.fr/monde/2013/06/30/berlin-et-bruxelles-tirent-les-grandes-oreilles-de-l-amerique_914864/ consulté le 20 avril 2020.

V. VICARD, « Vers la fin de la mondialisation », *ENS Lyon*, 3 janvier 2023, en ligne à URL : <https://ses.ens-lyon.fr/articles/vers-la-fin-de-la-mondialisation> consulté le 2 août 2023.

Vie publique, « Un accord commercial UE-Japon : entrée en vigueur le 1^{er} février 2019 », 30 janvier 2019, en ligne à URL : <https://www.vie-publique.fr/en-bref/20103-accord-commercial-ue-japon-entree-en-vigueur-le-1er-fevrier-2019> consulté le 10 juin 2023.

Vie publique, « Loi du 5 août 2021 relative à la gestion de la crise sanitaire », Panorama des lois, 6 août 2021, en ligne à URL : <https://www.vie-publique.fr/loi/280798-loi-5-aout-2021-vaccination-obligatoire-pass-sanitaire-crise-covid-19> consulté le 31 juillet 2023

A. VILLARREAL, “ Iconic TWA Flight Center Open to the Public for What May Be the Last Time ”, *Observer*, 10 octobre 2014, en ligne à URL : <https://observer.com/2014/10/twa-flight-center-open-to-the-public-for-what-may-be-the-last-time/> consulté le 30 août 2023.

Vosges matin, « Fichier des passagers : la Commission européenne prête à modifier sa proposition », , *Terrorisme*, 21 janvier 2015, en ligne à URL : <https://www.vosgesmatin.fr/actualite/2015/01/21/fichier-des-passagers-la-commission-europeenne-prete-a-modifier-sa-proposition> consulté le 24 août 2023.

The White House, “Fact Sheet: U.S.-EU Cyber Cooperation”, Office of the Press Secretary, 2014, en ligne à URL : <https://obamawhitehouse.archives.gov/the-pressoffice/2014/03/26/fact-sheet-us-eu-cyber-cooperation>, consulté le 23 septembre 2023.

WHO, « Statement on the fifteenth meeting of the IHR (2005) Emergency Committee on the COVID-19 pandemic », *Statement*, 5 mai 2023, en ligne à URL : [https://www.who.int/news/item/05-05-2023-statement-on-the-fifteenth-meeting-of-the-international-health-regulations-\(2005\)-emergency-committee-regarding-the-coronavirus-disease-\(covid-19\)-pandemic](https://www.who.int/news/item/05-05-2023-statement-on-the-fifteenth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic) consulté le 24 juillet 2023.

20 Minutes, « Coronavirus : La Chine utilise des lunettes connectées pour détecter les personnes à risque », *Le Monde*, High-Tech, 27 mars 2020, en ligne à URL : <https://www.20minutes.fr/monde/2749611-20200327-coronavirus-chine-utilise-lunettes-connectees-detecter-personnes-risque> consulté le 21 juillet 2023.

RÉFÉRENCES NORMATIVES

1. TEXTES JURIDIQUES FRANÇAIS

A. Textes législatifs

Loi n° 86-1020 du 9 septembre 1986 relative à la lutte contre le terrorisme.

Loi n° 2004-809 du 13 août 2004 relative aux libertés et responsabilités locales.

Loi n° 2005-357 du 20 avril 2005 relative aux aéroports.

Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^e siècle.

Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

La loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.

Loi n° 2021-689 du 31 mai 2021 relative à la gestion de la sortie de crise sanitaire.

Loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire.

Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.

B. Textes réglementaires

Article R. 232-12 du Code de la Sécurité Intérieure.

C. Codes

Code pénal, Livre IV : Des crimes et délits contre la nation, l'État et la paix publique, articles 410-1 à 450-5.

Code de la sécurité intérieure, article L. 111-1.

Code monétaire et financier, article L. 561-26.

Code des transports, article L. 6211-4.

Code des transports, article 6323-1.

2. TEXTES EUROPÉENS

A. Conseil de l'Europe

La Convention européenne des droits de l'Homme et des libertés fondamentales (ou Convention de sauvegarde des droits de l'homme et des libertés fondamentales), 1950.

Council of Europe, *The protection of individuals with regard to automatic processing of personal data in the context of profiling*, Recommendation CM/Rec (2010) 13 and explanatory memorandum, Council of Europe, 23 November 2010.

B. Union européenne

a. Traités

Traité instituant la Communauté européenne du charbon et de l'acier, Paris, 1951.

Traité sur le fonctionnement de l'Union européenne, Rome, 1958.

Traité instituant la Communauté européenne, Nice, 1995.

Traité sur l'Union européenne, Amsterdam, 1997.

Traité instituant la Communauté européenne, Lisbonne, 2007.

b. Documents du Conseil européen

Conseil européen, « Déclaration des membres du Conseil européen sur la lutte contre le terrorisme », Communiqué de presse, 12 février 2015 ; en ligne sur : <https://www.consilium.europa.eu/fr/press/press-releases/2015/02/12/european-council-statement-fight-against-terrorism/>

Conseil européen, « L'action de l'UE face au terrorisme », Politiques, 15 décembre 2022 ; en ligne sur : <https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/>

c. Règlements de l'Union européenne

Règlement n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JOUE n° L 8 du 12.1.2001, p. 1.

Règlement n° 216/2008 du Parlement européen et du Conseil, 20 février 2008, JOUE n° L 79, 19 mars, concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence européenne de la sécurité aérienne, et abrogeant la Directive n° 91/670 du

Conseil, le Règlement n° 1592/2002 et la Directive n° 2004/36, tel que modifié, en dernier lieu, par le Règlement n° 6/2013 de la Commission, 8 janvier 2013, JOUE n° L 4, 9 janvier.

Règlement n° 679/2016 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).

Règlement (UE) 2018/302 du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n° 2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE, article 1. Règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19.

d. Directives de l'Union européenne

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

Directive 2004/38 du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres.

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

Directive 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.

Directive 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.

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans

l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972 et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

e. Documents de la Commission européenne

Commission européenne, Décision 2004/535/CE du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique, *JOUE* L 235/11, 6 juill., p. 11.

Commission européenne, « Résumé de l'analyse d'impact », Document de travail des services de la commission accompagnant la Décision-cadre du Conseil relative à relative à l'utilisation de données des dossiers passagers (Passenger Name Record - PNR) à des fins répressives, Com(2007), 654 final, 2007.

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

Commission européenne, « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », 4 novembre 2010, COM(2010), 609 final, p. 20 ; en ligne sur : https://edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_fr

Commission européenne, Rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Rapport 2011 sur l'application de la charte des droits fondamentaux de l'Union européenne, SEC(2011), 567 final, 6 mai 2011.

Commission européenne, Proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure, COM(2011) 807 final, 23 novembre 2011.

Commission européenne, Document de la Commission COM (2014) 458 final du 10 juillet 2014, Rapport de la Commission au Parlement européen et au Conseil sur l'examen conjoint de la mise en œuvre de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières.

Commission européenne, Rapport de la Commission au Parlement européen et au Conseil sur le réexamen de la directive 2016/681 relative à l'utilisation des données des dossiers

passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

Commission européenne, Report from the Commission to the European Parliament and the Council, Bruxelles, 19 janvier 2017.

Commission européenne, *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield*, {SWD(2017) 344 final}, 18 octobre 2017.

Commission, Décision d'exécution (UE) 2019/419 de la Commission constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Japon en vertu de la loi sur la protection des informations à caractère personnel, 23 janvier 2019.

Commission européenne, Recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et le Japon aux fins du transfert et de l'utilisation de données des dossiers passagers (PNR) afin de prévenir et de combattre le terrorisme et d'autres formes graves de criminalité transnationale, 27 septembre 2019.

Commission européenne, « Décennie numérique de l'Europe: objectifs numériques pour 2030 », 2022 ; en ligne sur : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr

f. Documents du Parlement européen

Parlement européen, Rapport de la Commission des libertés et des droits des citoyens, de la justice et des affaires du 7 avril 2004, accompagné de l'avis de la Commission des affaires étrangères, des droits de l'Homme, de la sécurité commune et de la politique de défense des 5-6 avril 2004 (A5-0271/2004).

Parlement européen, Résolution du Parlement européen du 12 juillet 2007 sur l'accord avec les États-Unis d'Amérique concernant l'utilisation de données des dossiers des passagers aériens (PNR), 12 juillet 2007.

Parlement européen, Résolution du Parlement européen du 5 mai 2010 sur le lancement des négociations sur les accords relatifs aux données des passagers aériens (PNR) avec les États-Unis, l'Australie et le Canada, 5 mai 2010.

Parlement européen, Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, Les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures, le 12 mars 2014.

Parlement européen, Résolution du Parlement européen du 25 octobre 2018 sur l'exploitation des données des utilisateurs de Facebook par Cambridge Analytica et les conséquences en matière de protection des données (2018/2855(RSP)), (2020/C 345/10), 25 octobre 2018.

Règlement intérieur du Parlement européen, Parlement européen, juillet 2022.

g. Documents du Conseil de l'Union européenne

Conseil de l'Union européenne, « La stratégie européenne de lutte contre le terrorisme », 2005 ; en ligne sur : <https://www.consilium.europa.eu/fr/policies/fight-against-terrorism/eu-strategy/>

Conseil de l'Union européenne, Décision 2006/230 du Conseil de l'Union européenne, 18 juillet 2005, relative à la conclusion de l'accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données IPV/DP, JOUE n° L 82.

Conseil de l'Union européenne, Décision 2012/472 du Conseil de l'Union européenne, 26 avril 2012, relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, JOUE n° L 215.

Conseil de l'Union européenne, « Évaluation à mi-parcours du programme de Stockholm », Note, Bruxelles, 13 novembre 2012 ; en ligne sur : <http://www.gdr-elsj.eu/wp-content/uploads/2012/12/Doc-15921.12-Evaluation-Stockholm.pdf>

h. Documents du Comité européen de la protection des données (anciennement Groupe de travail « Article 29 »)

Groupe « Article 29 », Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis (11647/02/FR/Final).

Groupe « Article 29 », Avis 4/2003 du 13 juin 2003, sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers 11070/03/FR.

Groupe « Article 29 », Avis 2/2004 du 29 janvier 2004, sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (US CBP) (10019/04/FR).

Groupe « Article 29 », Avis commun sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR), à des fins répressives, présentée par la Commission le 6 novembre 2007.

Groupe « Article 29 », Avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, adopté le 12 novembre 2010, WP 178. V. le II, p. 3.

Groupe « Article 29 », Avis 10/2011 sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers 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 (00664/11/EN, WP 181).

Groupe « Article 29 », Avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif du 27 février 2014 (536/14/FR, WP 211).

Groupe « Article 29 », Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, 6 février 2018.

EDPB, "EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain", News, EDPB, 28 February 2023.

i. Documents du Contrôleur européen de la protection des données

Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion d'un accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations anticipées sur les voyageurs (API)/dossiers passagers (PNR), (2005/C 218/06), 15 juin 2005.

Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure, 9 décembre 2011, JOUE n° C 35, 9 février 2012, p. 16, § 10, résumé de l'avis en ligne à URL : https://www.edps.europa.eu/sites/default/files/publication/13-09-30_canada_ex_sum_fr.pdf consulté le 27 mai 2024.

Avis du Contrôleur européen de la protection des données, 9 décembre 2011, sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure : JOUE n° C 35, 9 février 2012, p. 16, §10.

CEPD, « Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the

European Union on the transfer and processing of Passenger Name Record data », 30 septembre 2013, considérant 3.

CEPD, « La stratégie du CEPD 2015-2019 », 2015 ; en ligne sur : https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_fr.pdf

Avis du Contrôleur européen de la protection des données sur le mandat de négociation d'un accord entre l'UE et le Japon pour le transfert et l'utilisation de données des dossiers passagers, 6/2019, 25 octobre 2019 ; en ligne sur : https://edps.europa.eu/sites/default/files/publication/19-10-25_opinion_recommendation_pnr_japan_fr.pdf

Avis du Contrôleur européen de la protection des données sur les propositions de décisions du Conseil relatives à la conclusion et à la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, C 51/12, 22 février 2014 ; en ligne sur : https://www.edps.europa.eu/sites/default/files/publication/13-09-30_canada_ex_sum_fr.pdf

3. TEXTES INTERNATIONAUX

A. Traités

Convention relative à l'aviation civile internationale, 7 décembre 1944, Chicago (Organisation de l'aviation civile internationale, Guidelines on Passenger Name Record).

WCO/IATA/ICAO API Liaison Committee, XML Implementation Guidelines – PNR Data Pushing to States or Other Authorities – PNRGOV, octobre 2013.

IATA, *Passenger and airport data interchange standards*, PADIS XML Implementation Guide, PNRGOV Message, 2016 ; en ligne sur : https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/pnrgov20xml20implementation20guide2016_1.pdf

B. Accords PNR

Accord entre les États-Unis d'Amérique et l'Union européenne sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure ("DHS") (accord PNR 2007) 11595/07, 18 juillet 2007.

Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure, Bruxelles, 14 décembre 2011.

Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au Ministère américain de la sécurité intérieure, *Journal officiel* n° L 0215 du 11/08/2012.

Accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, (12657/2013), 2013.

C. Comité des droits de l'Homme (Nations-Unies)

Comité des droits de l'Homme, *Coeriel and Aurik v. the Netherlands* (1994), Communication n° 453/1991.

D. Conseil de Sécurité (Nations-Unies)

Conseil de sécurité, Résolution 1624, (2005), ONU.

Conseil de sécurité, Résolution 2253, (2015), ONU.

Conseil de sécurité, Résolution 2396, (2017), ONU.

4. RÉFÉRENCES JURIDIQUES ÉTRANGÈRES

A. Algérie

R. ARADJI, « Loi n°18-07 : Protection des données personnelles », Groupement Algérien des Acteurs du Numérique, 2020 ; en ligne sur : <https://www.gaan.dz/articles-divers/loi-n18-07--protection-des-donnees-personnelles-page-115653>

B. Arabie saoudite

A. LECLAIRE, « La "personal data protection law" d'Arabie saoudite », *Village de la justice*, 1^{er} août 2022 ; en ligne sur : <https://www.village-justice.com/articles/personal-data-protection-law-arabie-saoudite,43326.html#:~:text=A%20l'instar%20de%20quelques,vigueur%20le%2017%20mars%202023>

C. Bahreïn

DLAPIPER, “Bahrain”, *Data protection law of the world*, 2023 ; en ligne sur : <https://www.dlapiperdataprotection.com/index.html?t=law&c=BH>

D. Égypte

Data Guidance, 2022 ; en ligne sur : <https://www.dataguidance.com/notes/egypt-data-protection-overview>

E. Émirats Arabes Unis

M. WHITE, P. MENNIE, O. SYKES, R. CHUDZYNKSI, “Data privacy handbook for the United Arab Emirates”, *PWC*, 2021.

F. États-Unis

U.S. Department of Homeland Security, U.S. Customs and Border Protection Passenger Name Record Privacy Policy.

California Consumer Privacy Act of 2018, CAL. CIV. CODE, § 1789.100 - 1789.199.

Executive Order 14086 Enhancing Safeguards for United States Signals Intelligence, 7 october 2022.

Section 702 FISA et Executive Order 12 333.

Department of Homeland Security, “Fact Sheet: US-EU Passenger Name Record Agreement Signed”, 28 mai 2004.

G. Japon

Constitution du Japon, promulguée le 3 novembre 1946, entrée en vigueur le 3 mai 1947, en ligne sur : <https://mjp.univ-perp.fr/constit/jp1946.htm>

H. Jordanie

DLAPIPER, “Jordan”, *Data protection law of the world*, 19 janvier 2023 ; en ligne sur : <https://www.dlapiperdataprotection.com/index.html?t=law&c=JO&c2=>

I. Koweït

DLAPIPER, “Kuwait”, *Data protection law of the world*, 22 décembre 2022 ; en ligne sur : <https://www.dlapiperdataprotection.com/index.html?t=law&c=KW>

J. Lybie

DLAPIPER, “Lybie”, *Data protection law of the world*, 13 janvier 2023 ; en ligne sur : <https://www.dlapiperdataprotection.com/index.html?t=law&c=LY&c2=>

K. Maroc

Direction générale de la sécurité des systèmes d'information, Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ; en ligne sur : <https://www.dgssi.gov.ma/fr/content/loi-09-08-relative-la-protection-des-personnes-physiques-l-egard-du-traitement-des-donnees-caractere-personnel.html#:~:text=Cette%20loi%20vise%20%C3%A0%20assurer,de%20ses%20partenaires%20notamment%20europ%C3%A9ens>

L. Oman

Data Guidance, 2022 ; en ligne sur : <https://www.dataguidance.com/news/oman-data-protection-law-comes-force#:~:text=Royal%20Decree%20No.,1429%2C%20on%2013%20February%202022,>

M. Qatar

Data Guidance, 2022 ; en ligne sur : <https://www.dataguidance.com/jurisdiction/qatar-financial-centre>

JURISPRUDENCE

1. JURIDICTIONS FRANÇAISES

A. Conseil d'État

Conseil d'État, n° 271569, *ministère de l'Intérieur et de l'aménagement du territoire c/ Société Air France, Lebon*, AJDA 2006, 754, concl. I. de Silva, 7 déc. 2005.

Conseil d'État, Assemblée générale, Avis n° 390866 sur le projet de loi constitutionnelle de la protection de la Nation, 11 décembre 2015.

B. Cours administratives d'appel

Cour administrative d'appel Paris, 10 févr. 1998, n° 96PA02799, *Compagnie nationale Air France, Lebon*, AJDA 1998, 280 ; et 227.

Cour administrative d'appel Paris, 12 avr. 2010, n° 08PA05060, *ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales c/ Société V. Ships*, AJDA 2010, 1446.

C. Cour de cassation

Cour de Cassation, Chambre criminelle, 19 février 1997, n° 95-81352.

D. Conseil constitutionnel

Conseil constitutionnel, décision n° 2019-781 DC du 16 mai 2019 concernant la loi relative à la croissance et la transformation des entreprises.

E. Commission nationale de l'informatique et des libertés

CNIL, Délibération n° 2021-004 du 14 janvier 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19.

CNIL, Délibération n° 2021-139 du 21 octobre 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 (mai à septembre 2021).

2. JURIDICTIONS EUROPÉENNES

1. Cour européenne des droits de l'Homme

CEDH, n° 30562/04 et 30 566/04, *Marper c/ Royaume-Uni*, 4 décembre 2008.

CEDH, n° 38334/08, *Anchev c/ Bulgarie*, 11 janvier 2018.

Cour de justice de l'Union européenne (anciennement CJCE)

CJCE, *R. & V. Haegeman c/ État belge*, affaire C-181-73, 30 avril 1974.

CJCE, *Jean Noël Royer*, affaire C-48/75, 8 avril 1976.

CJCE, *Parlement c/ Conseil et Commission*, affaire C-181/91 et C-6248/91, Rec. I. 3685, 30 juin 1993.

CJCE, *Parlement européen c/ Conseil de l'Union européenne et Commission des Communautés européennes*, affaire C-317/04, Rec. I-04721s, 30 mai 2006.

CJUE, *Volker und Markus Schecke GbR (C-92/09) et Hartmut Eifert (C-93/09) c/ Land Hessen*, (pt 52), 9 novembre 2010.

CJUE, *Land Baden-Württemberg c/ Panagiotis Tsakouridis*, affaire C-145/09, 23 novembre 2010.

CJUE, *Digital Rights Ireland Ltd c/ Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, affaires jointes C-293/12 et C-594/12, 8 avril 2014.

CJUE, *Parlement européen c/ Conseil*, affaire C-658-11 relatif au jugement de pirates arrêtés par la force Eunavfor Atalanta, 24 juin 2014.

CJUE, *Maximillian Schrems c/ Data Protection Commissioner*, affaire C-362/14, 6 octobre 2015.

CJUE, *Tele2 Sverige AB c/ Post- och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson e.a.*, affaires jointes C-203/15 et C-698/15, 21 décembre 2016.

CJUE, avis 1/15 de la Cour (grand chambre), 26 juillet 2017.

CJUE, arrêt de la Cour (grande chambre), *Ligue des droits humains c/ Conseil des ministres*, affaire C-817/19. 21 juin 2022.

CJUE, conclusions de l'avocat Général M. Giovanni Pitruzzella, affaire C-817/19, *Ligue des droits humains c/ Conseil des ministres*, 27 janvier 2022.

INDEX

Aéroport... 20, 21, 26, 33, 38, 108, 110, 120, 137, 185, 274, 275, 285, 286, 300, 302, 313, 314, 315, 316, 317, 318, 320, 324, 326, 327, 330, 339, 340, 344, 348, 352, 395, 415, 436.	Frontières..... 24, 34, 40, 47, 49, 54, 56, 58, 62, 68, 74, 76, 84, 92, 97, 103, 113, 116, 121, 127, 128, 132, 139, 142, 151, 158, 173, 189, 201, 229, 256, 259, 260, 263, 264, 267, 275, 282, 289, 292, 309, 311, 314, 316, 346, 348, 349, 356, 357, 394, 407, 413, 424, 434, 462.
Automated Targeting System..... 60, 62.	IATA..... 55, 152, 297, 329, 381, 382, 440.
Australie..... 40, 85, 150, 151, 152, 378.	ICAO..... 24, 55, 280, 381, 382, 383.
Big Data..... 183, 264, 266, 302, 410.	Internet des objets..... 310, 328, 329.
Biométries..... 58, 257, 268, 331, 332, 338, 350, 351, 352.	Japon..... 171, 244, 245, 248, 250, 451.
California Consumer Privacy Act... 62, 73.	Lutte contre le terrorisme..... 29, 37, 43, 44, 48, 53, 57, 64, 67, 103, 114, 116, 119, 130, 151, 180, 197, 203, 221, 265, 270, 297, 298, 300, 307, 330, 362, 390, 460.
Canada..... 37, 40, 47, 85, 114, 146, 149, 150, 157, 177, 184, 196, 202, 220, 242, 287, 331, 332, 378, 445, 451.	Multilatéralisme..... 245, 357, 417, 436, 441, 442, 444, 446, 447, 455.
Charte des droits fondamentaux..... 83, 84, 89, 137, 139, 145, 148, 153, 159, 174, 180, 185, 196, 204, 211, 219, 220, 251, 286, 302, 318, 363, 375, 398.	Patriot Act..... 2, 64, 66.
Collecte de données..... 22, 24, 30, 33, 36, 40, 55, 59, 65, 74, 89, 92, 118, 124, 128, 130, 135, 137, 143, 150, 160, 166, 173, 183, 191, 225, 228, 236, 240, 244, 250, 260, 270, 272, 290, 411, 442, 461, 463.	Parlement européen..... 26, 30, 35, 41, 65, 77, 82, 88, 89, 90, 92, 94, 120, 128, 133, 137, 148, 151, 152, 175, 176, 192, 198, 207, 208, 210, 211, 217, 224, 232, 235, 238, 248, 259, 272, 276, 282, 310, 378, 379, 453, 460.
Contrôleur européen de la protection des données..... 47, 83, 137, 143, 150, 197, 203, 207, 214, 223, 224, 231, 233, 234, 236, 249, 253, 261, 287, 296, 298, 331, 345, 379, 402, 461.	Prism (affaire)..... 64, 65, 66, 370.
Comité européen sur la protection des données..... 7, 195, 207, 214, 222, 227, 239, 404.	Privacy Act (US)..... 71, 87.
	Privatisation..... 311, 316, 328, 328, 334, 335, 337, 338, 339, 340, 345, 348, 352, 357, 364.
	Profilage... 57, 155, 265, 288, 290, 295, 463.
	Règlement général sur la protection des données..... 24, 35, 125, 149, 207, 211, 222, 256, 267, 287, 292, 296, 369.
	Sécurité collective..... 30, 31, 35, 38, 47,

Commission nationale de l'informatique et des libertés..... 58, 75, 183, 211, 214, 239, 266, 293, 331, 351, 363, 375, 376, 424, 453.	73, 83, 117, 127, 135, 182, 192, 196, 203, 220, 253, 271, 361, 379, 380, 428, 434, 451.
Cour de justice de l'Union européenne..... 39, 103, 138, 140, 142, 150, 153, 157, 159, 161, 176, 179, 184, 186, 187, 196, 201, 204, 218, 219, 303, 363, 367, 372, 376, 392, 397, 433, 445, 451, 459, 460.	Shrems (arrêt)..... 153, 159, 213, 363, 371, 376, 398, 451.
Covid-19..... 21, 256, 301, 334, 352, 358, 408, 410, 412, 413, 414, 422, 424, 466.	Surveillance..... 32, 39, 64, 66, 75, 95, 130, 132, 180, 197, 213, 227, 260, 277, 301, 349, 433, 452, 462.
Customs and Border Protection..... 54, 58, 59, 74, 200, 380.	Territoire..... 26, 45, 50, 88, 156, 175, 245, 257, 258, 279, 280, 284, 285, 307, 311, 357, 407, 425, 430, 465, 466.
Data Privacy Framework..... 13, 226.	Transport..... 19, 20, 23, 36, 51, 131, 135, 138, 142, 147, 195, 260, 271, 273, 279, 282, 298, 318, 329, 334, 353, 379.
Directive PNR..... 27, 33, 138, 140, 208, 297, 364, 392, 405.	Transfert des données..... 3, 58, 75, 83, 88, 93, 117, 150, 158, 160, 177, 180, 187, 229, 237, 298, 366, 369, 373, 379, 390, 445, 453.
Dossiers passagers..... 27, 38, 86, 108, 116, 125, 134, 140, 148, 155, 161, 192, 206, 214, 231, 239, 244, 251, 256, 258, 262, 266, 271, 286, 304, 313, 315, 325, 331, 348, 358, 362, 367, 380, 386, 394, 401, 404, 412, 424, 431, 438, 440, 448, 452, 458, 461.	Unité Information Passager..... 131, 134, 303, 307, 364, 382, 384, 385, 386, 443.
Droits fondamentaux.... 33, 84, 89, 94, 103, 137, 145, 175, 184, 201, 207, 213, 225, 229, 271, 293, 300, 303, 393, 459, 461.	Vie privée..... 2, 24, 28, 30, 44, 90, 160, 226, 227, 269, 392, 430, 431.
États-Unis..... 29, 46, 50, 64, 70, 78, 79, 87, 93, 98, 106, 113, 118, 121, 141, 147, 201, 213, 226, 237, 249, 283, 318, 361, 366, 371, 375, 385, 389, 412, 444, 448, 450, 454, 460.	Voyageurs..... 20, 23, 25, 36, 55, 59, 61, 106, 110, 123, 134, 172, 175, 184, 202, 236, 241, 257, 265, 283, 284, 286, 298, 300, 309, 316, 320, 330, 335, 347, 352, 384, 387, 394, 399, 413, 423, 427, 428.
Foreign Intelligence Surveillance Act..... 66, 228, 452.	
France..... 25, 43, 48, 53, 81, 91, 101, 166, 181, 191, 199, 245, 259, 266, 270, 285, 290, 301, 319, 321, 338, 358, 412, 422, 449, 461.	

Table des matières détaillée

Résumé / Summary.....	9
Sommaire.....	11
Principaux acronymes et sigles.....	13
Introduction générale.....	19
Section 1 – L’intérêt accru du secteur du transport aérien pour les données personnelles	23
Section 2 – Les dossiers passagers, un outil de lutte contre les infractions terroristes et transnationales	26
Section 3 – Les données personnelles des dossiers passagers, sujet de frictions entre deux libertés fondamentales	29
Partie I – Les limites traditionnelles à la protection juridique des dossiers passagers.....	35
Titre 1 – La prééminence des législations répressives en matière de dossiers passagers.....	39
Chapitre 1 – L’antagonisme entre les législations répressives relatives à la transmission des dossiers passagers.....	43
Section 1 – L’obligation de transmission imposée par le droit américain.....	48
Sous-section 1 – Une rupture dans le droit pénal américain.....	49
Sous-section 2 – Une conception intrusive des dossiers passagers.....	70
Section 2 – La contestation opposée par le droit européen.....	81
Sous-section 1 – Une contestation institutionnelle sans conséquences juridiques.....	81
Sous-section 2 – Une contestation limitée réalisme politique.....	87
Chapitre 2 – Le consensus des législations répressives sur la finalité sécuritaire des dossiers passagers.....	101
Section 1 – Un consensus illustré par l’existence d’un accord euro-américain sur le transfert des dossiers passagers.....	103
Sous-section 1 – L’influence américaine originelle de l’usage sécuritaire des dossiers passagers.....	105

Sous-section 2 – Un accord euro-américain essentiellement sécuritaire.....	113
Section 2 - La présence de la logique répressive américaine dans la directive européenne sur les dossiers passagers.....	126
Sous-section 1 – Une directive européenne reprenant la préoccupation américaine vis-à-vis des infractions terroristes.....	128
Sous-section 2 – Une directive européenne reléguant la protection des droits fondamentaux.....	133
Titre 2 – L’empiètement des législations répressives sur les droits fondamentaux des passagers aériens.....	141
Chapitre 1 – Les accords PNR, un échange des dossiers passagers sans protection juridique effective.....	145
Section 1 – L’empiètement reconnu sur le droit au respect à la vie privée et sur le droit à la protection des données personnelles.....	148
Sous-section 1 – Un accord PNR euro-canadien objet de contestation.....	149
Sous-section 2 – L’absence de développement d’accords PNR avec les pays de la Ligue arabe.....	161
Section 2 – La limitation des droits fondamentaux au nom de la sécurité publique.....	174
Sous-section 1 – Une limitation fondée sur une interprétation originale de la « loi ».....	176
Sous-section 2 – Une limitation fondée sur un objectif d’intérêt général.....	178
Sous-section 3 – Une limitation des droits fondamentaux au caractère disproportionné.....	180
Chapitre 2 – Les institutions européennes, une protection juridique déséquilibrée des dossiers passagers.....	189
Section 1 – Des acteurs initiateurs d’un cadre juridique favorable à la sécurité publique : le Conseil de l’Union européenne et la Commission.....	191
Sous-section 1 – Le Conseil de l’Union européenne, promoteur de la sécurité collective.....	192
Sous-section 2 – La Commission, l’organe négociateur des accords PNR.....	198

Section 2 – Des acteurs garants des droits fondamentaux des passagers aériens : le Parlement européen, la Cour de justice de l’Union européenne, le Comité européen de la protection des données et le Contrôleur européen de la protection des données.....	207
Sous-section 1 – Le Parlement européen, une institution impliquée dans la protection des droits fondamentaux.....	207
Sous-section 2 – La Cour de justice de l’Union européenne, garante du droit fondamental à la protection des données personnelles.....	216
Sous-section 3 – Le Comité européen de la protection des données, le garant d’un nouvel ordre.....	221
Sous-section 4 – Le Contrôleur européen de la protection des données, une autorité de contrôle indépendante investie dans la protection des droits fondamentaux.....	231
Conclusion de la première partie.....	253
Partie II – Les nouvelles menaces sur la protection juridique des dossiers passagers.....	255
Titre 1 – L’affaiblissement de la protection juridique des dossiers passagers dans leur traitement aux frontières.....	259
Chapitre 1 – L’affaiblissement de la protection juridique des dossiers passagers par la collecte de données personnelles aux frontières.....	263
Section 1 – Une opération de collecte massive des données personnelles des passagers aériens.....	266
Sous-section 1 – Le droit européen face à la collecte massive des données personnelles.....	267
Sous-section 2 – Les transporteurs aériens face à la collecte massive des données personnelles des passagers aériens.....	278
Section 2 – Un profilage des passagers aériens en conflit avec le droit à la vie privée et la protection des données personnelles.....	287
Sous-section 1 – Le profilage face aux règles régissant le traitement des données à caractère personnel.....	289
Sous-section 2 – Le profilage face aux règles régissant le traitement des données personnelles des passagers aériens.....	296

Chapitre 2 – L’affaiblissement de la protection juridique des dossiers passagers par le rôle des acteurs privés dans les aéroports.....	309
Section 1 – L’ingérence contestée des acteurs privés dans le traitement des dossiers passagers aux frontières.....	311
Sous-section 1 – La participation accrue des acteurs privés dans la gestion des aéroports.....	311
Sous-section 2 – Les défis du traitement des données aux frontières au regard de l’ingérence des acteurs privés.....	316
Section 2 – La mise en danger de la protection juridique des dossiers passagers par la privatisation des aéroports.....	327
Sous-section 1 – La transformation contemporaine des aéroports par les nouvelles technologies.....	327
Sous-section 2 – La protection des données personnelles des passagers aériens face à la privatisation des aéroports.....	337
Titre 2 – L’affaiblissement de la protection juridique des dossiers passagers par la déterritorialisation.....	355
Chapitre 1 – Une déterritorialisation par le caractère supranational des dossiers passagers : l’effacement du droit national dans les transferts de données personnelles.....	359
Section 1 – Le transfert des dossiers passagers : l’extension de l’extraterritorialité au détriment d’un espace protecteur des droits des passagers.....	361
Sous-section 1 – La multiplication des actes juridiques privilégiant la fluidité des transferts transnationaux des données à caractère personnel.....	364
Sous-section 2 – L’encadrement juridique du transfert transfrontalier des données à caractère personnel des passagers aériens.....	376
Section 2 – Le stockage des dossiers passagers : une fragile limitation temporelle au profit de la conservation des données personnelles des passagers aériens.....	391
Sous-section 1 – La conservation des données à caractère personnel, un enjeu crucial pour le droit européen.....	391
Sous-section 2 – La conservation des données des passagers aériens, un équilibre entre sécurité et liberté difficilement mis en œuvre.....	398

Chapitre 2 – Une déterritorialisation limitée par l’implication des États dans les crises contemporaines : le retour du droit national dans l’utilisation des données personnelles.....	405
Section 1 – Vers une probable extension par les États du champ d’application des dossiers passagers à la santé : une conséquence de la crise du coronavirus.....	408
Sous-section 1 – La crise du coronavirus, des solutions mettant en danger les données à caractère personnel des passagers aériens.....	410
Sous-section 2 – L’utilisation des données personnelles contre la propagation de la pandémie comme une confirmation de l’extension du domaine des données personnelles des passagers aériens.....	420
Section 2 – Vers une harmonisation difficile du régime national des dossiers passagers : une conséquence de la crise du multilatéralisme.....	434
Sous-section 1 – La protection juridique des dossiers passagers face à une myriade d’accords caractérisés par un défi d’harmonisation.....	436
Sous-section 2 – Les législations des dossiers passagers au défi de l’harmonisation.....	444
Conclusion de la seconde partie.....	455
Conclusion générale.....	457
Bibliographie.....	465
Références normatives.....	517
Jurisprudence.....	529
Index.....	531
Table des matières détaillée.....	533