UNIVERSITÉ D'AIX-MARSEILLE

FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

PÔLE TRANSPORTS

INSTITUT DE FORMATION UNIVERSITAIRE ET DE RECHERCHE DU TRANSPORT AÉRIEN

L'EFFICIENCE DU DROIT À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE DE LA MISE EN PLACE DE L'ETIAS

Mémoire pour l'obtention du

Master 2 Droit et Management du Transport Aérien

Par

Isra BENDJEMA

Sous la direction de Mme le professeur Julie LABORDE DIT BOURIAT

et Madame Elodie MUNIER

Année universitaire 2020-2021

UNIVERSITÉ D'AIX-MARSEILLE

FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

PÔLE TRANSPORTS

INSTITUT DE FORMATION UNIVERSITAIRE ET DE RECHERCHE DU TRANSPORT AÉRIEN

L'EFFICIENCE DU DROIT À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE DE LA MISE EN PLACE DE L'ETIAS

Mémoire pour l'obtention du

Master 2 Droit et Management du Transport Aérien

Par

Isra BENDJEMA

Sous la direction de Mme le professeur Julie LABORDE DIT BOURIAT

et Madame Elodie MUNIER

Année universitaire 2020-2021

REMERCIEMENTS

Je souhaite tout d'abord remercier Madame LABORDE DIT BOURRIAT qui m'a donné l'opportunité de suivre cette formation, ainsi que tous les intervenants qui ont pris du temps pour nous partager leurs connaissances, leurs expériences et pour tous les conseils avisés.

Je remercie également Marjorie, Lia et Stéphanie pour leur accompagnement tout au long de cette année si particulière.

Je remercie chaleureusement Maryn BAZARD, Elodie MUNIER et Mathilde DEMAY qui m'ont accordé leur confiance, leur bienveillance et du temps durant cette année d'alternance riche en apprentissage. Merci à Laura SALABERT pour son aide et ses conseils qui ont été précieux. Enfin, merci à Thibault GUENOLE, avec qui j'ai partagé cette formidable expérience.

Enfin, je tiens particulièrement à remercier Lucas GAUDIERE pour son soutien indéfectible, ses encouragements et sa patience.

SOMMAIRE

REMERCIEMENTS **2**

GLOSSAIRE **6**

INTRODUCTION **9**

PARTIE I – LES DÉFIS DE LA SÛRETÉ ET DE LA SÉCURITÉ DES FRONTIÈRES EXTÉRIEURES EN EUROPE À SURMONTER **17**

Titre I - La nécessité d'un système électronique d'autorisation de voyage **17**

Chapitre I. La remise en cause du système actuel de l'espace Schengen 17

Chapitre II. Les mutations engendrées par un système électronique d'autorisation de voyage 31

Titre II - Des systèmes d'information collectant un nombre grandissant de données à caractère personnel **43**

Chapitre I. La solution de l'interopérabilité des systèmes d'information 43

Chapitre II. Le rôle central et renforcé de l'agence européenne eu-LISA dans la gestion des données à caractère personnel 50

PARTIE II - LES ENJEUX DU DROIT À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL FACE AUX NOUVEAUX BESOINS DE SÉCURITÉ ET D'INFORMATION **55**

Titre I- La discutabilité de l'effectivité du droit à la protection des données à caractère personnel **55**

Chapitre I. L'évolution des grands principes du droit à la protection des données à caractère personnel 55

Chapitre II. Des principes et des droits confrontés à une ingérence au nom de la sécurité publique 71

Titre II- Un équilibre cornélien mais politique entre protection et sécurité **79**

Chapitre I. Entre approche économique et protectrice : les exemples étrangers 79

Chapitre II. Le développement d'outils pour une Europe qui protège : la sécurité numérique 89

CONCLUSION **101**

BIBLIOGRAPHIE **103**

TABLE DES MATIÈRES **116**

GLOSSAIRE

ADP	*Aéroports de Paris*
AESRI	*Agence Européenne chargée de la Sécurité des Réseaux et de l'Information*
ANSSI	*Agence Nationale de Sécurité des Systèmes d'Information*
APIS	*Advance Passenger Information System*
ARCEP	*Autorité de Régulation des Communications Electroniques, des postes et de la distribution de la presse*
AVE	*Autorisation de Voyage Electronique*
BVG	*Bureau Vérificateur Général*
c/	*Contre*
CAN	*Canadian Dollar*
CEDH	*Cour Européenne des Droits de l'Homme*
CEPD	*Contrôleur Européen de la Protection de Données*
CESEDA	*Code de l'Entrée et du Séjour des Etrangers et du Droit d'Asile*
CGV	*Conditions Générales de Vente*
CIA	*Central Intelligence Agency*
CIJ	*Cour Internationale de Justice*
CIL	*Correspondant Informatique et Libertés*
CJCE	*Cour de Justice de la Communauté Européenne*
CJUE	*Cour de Justice de l'Union Européenne*
CNIL	*Commission Nationale de l'Informatique et des Libertés*
CSIRT	*Computer Security Incident Response Team*
CyCLONe	*Cyber Crisis Liaison Organisation Network*
DCSSI	*Direction Centrale de la Sécurité des Systèmes d'Information*
ECRIS	*European Criminal Records Information System*
EES	*Système d'Entrée/Sortie*
ELSJ	*Espace de Liberté, de Sécurité, de Justice*
ENISA	*European Union Agency for Cybersecurity*
ESP	*European Search Portal*
ESTA	*Electronic System for Travel Authorization*
ETIAS	*European Travel Information Authorization System*
FIP	*Fair Information Practice*
FSI	*Fonds pour la Sécurité Intérieure*
IA	*Intelligence Artificielle*
ICO	*Information Commissioner's Office*
IFURTA	*Institut de Formation Universitaire et de Recherche du Transport Aérien*
INAD	*Passager INADmissible*

LPRPDE	*Loi sur la Protection des Renseignements Personnels et des Documents Electroniques*
LPVPC	*Loi sur la Protection de la Vie Privée des Consommateurs*
LSDA	*Loi sur la Sûreté des Déplacements Aériens*
NSA	*National Security Agency*
OACI	*Organisation de l'Aviation Civile Internationale*
OCDE	*Organisation pour la Coopération et le Développement Economique*
ONU	*Organisation des Nations Unies*
PARAFE	*Passage Automatisé Rapide aux Frontières Extérieures*
RGPD	*Règlement Général sur la Protection de Données*
SCRS	*Service Canadien du Renseignement de Sécurité*
SIS	*Système d'Information Schengen*
SLTD	*Stolen and Lost Travel Documents*
SRI	*Sécurité des Réseaux et des systèmes d'Information*
TDAWN	*Travel Documents Associated with Notices Database*
TFUE	*Traité sur le Fonctionnement de l'Union Européenne*
USD	*US Dollar*
v.	*Versus*
VIS	*Visa Information System*

INTRODUCTION

« Qu'on le veuille ou non, le monde est divisé en Etats-nations. Et le droit d'accueillir ou non les étrangers est une prérogative des Etats (...) car jusqu'à nouvel ordre, les Etats-nations existent, les frontières persistent, l'Etat de droit demeure »[1].

Patrick Weil

I. La notion complexe de frontière

Le Dictionnaire de terminologie du droit international définit la frontière comme étant une *« ligne déterminant où commencent et où finissent les territoires relevant respectivement de deux Etats voisins. ».* Cette notion née à partir du 17e siècle avec les premiers règlements frontaliers entre Etats et la naissance de l'Etat moderne.

Claude BLUMMAN, professeur de droit, souligne la proximité de cette notion avec celle du territoire, de l'Etat et de la Nation[2]. En effet, selon lui, la frontière est liée à un territoire qui marque sa limite et ce territoire est l'Etat. Ainsi, la frontière crée l'Etat. C'est d'ailleurs, l'un des éléments constitutifs de l'Etat, en vertu du droit international. La Nation est quant à elle une *« communauté politique établie sur un territoire défini et personnifiée par une autorité souveraine. »*[3]. Il existe autour de ce concept un débat doctrinal sur l'existence ou non d'une identité historique, culturelle, linguistique ou encore religieuse qui permettrait de caractériser la détermination de cette nation[4].

Jean-Marc SOREL, professeur de droit, considère qu'il n'existe pas de frontière naturelle et qu'elle est *« toujours la résultante d'une démarche réfléchie »*[5]. Il est vrai que la délimitation des frontières est expliquée par des raisons historiques et politiques. L'exemple de l'Alsace et la Lorraine en est une parfaite illustration. Sur les cartes géographiques, une délimitation claire est faite sur les chaînes de montagnes et cours d'eau. La détermination des frontières reste aujourd'hui un sujet fort en actualité qui fait l'objet de convoitise et de contestation.

---

[1] P. WEIL, Le Nouvel Observateur, 7-13 août 1997
[2] C. BLUMANN, « La Frontière », 1980
[3] Dictionnaire Larousse, 1996
[4] J-M. SOREL, « Frontière internationale », *Répertoire de droit international*, Juillet 2017
[5] J-M. SOREL, « Frontière internationale », *Répertoire de droit international*, Juillet 2017

Il existe plusieurs types de frontières : les frontières terrestres, maritimes et aériennes. Alors que la délimitation des premières n'est régie par aucun texte, les frontières maritimes découlent de règles fixées dans la Convention de Genève de 1958[6] et la Convention de Montego-Bay de 1982[7]. Quant aux frontières aériennes, les principes figurent dans la Convention de Paris de 1919[8] puis la Convention de Chicago de 1944[9].

Les frontières d'un Etat sont protégées par un régime juridique qui renvoie à deux notions fondamentales : l'inviolabilité et l'intangibilité des frontières[10].

Le principe d'inviolabilité des frontières, prévu par l'article 2 §4 de la Charte des Nations unis[11], est l'interdiction de franchir un Etat en ayant recours à la force armée afin d'atteindre sa souveraineté.

Le principe d'intangibilité des frontières rend impossible une quelconque remise en question des frontières déjà existantes, en vertu de la Convention de Vienne de 1969[12]. La locution *uti possidetis juris* signifie « vous posséderez ce que vous possédiez déjà ». Ce principe a été redéfini par la Cour International de Justice (ci-après « CIJ ») à l'occasion d'une affaire qui a opposé le Burkina Fasso et la République du Mali : *« le principe de l'intangibilité des frontières vise avant tout à assurer le respect des limites territoriales d'un Etat au moment de son indépendance. Si ces limites n'étaient que des limites entre divisions administratives relevant initialement de la même souveraineté, l'application du principe uti possidetis emporte leur transposition en frontières internationales proprement dites. »*[13]. Ainsi, les nouveaux Etats doivent respecter les frontières qui ont été fixés par leur prédécesseur. Cette nécessaire stabilité est rappelé par un l'arrêt Temple de Préah-Vihéar de 1962 de la CIJ[14].

Les frontières sont à la fois l'enjeu principal des accords Schengen mais c'est également la cause qui explique pourquoi cet espace est à un tournant de son existence.

[6] Convention des Nations Unies sur la mer territoriale et la zone contiguë, 29 avril 1958
[7] Convention des Nations Unies sur le droit de la mer, 10 décembre 1982
[8] Convention portant règlementation de la navigation aérienne, 13 octobre 1919
[9] Convention relative à l'aviation civile internationale, 07 décembre 1944
[10] Cours de Droit international des espaces et de l'environnement de Madame POIRAT Florence, année universitaire 2019-2020
[11] Charte des Nations unies du 26 juin 1945
[12] Convention de Vienne sur le droit des traités, 23 mai 1969
[13] CIJ, Burkina Fasso v. République du Mali, 1986, affaire 63
[14] CIJ, Cambodge v. Thaïlande, 1962, affaire 45

II. L'espace Schengen, à un tournant de son existence

La libre circulation des marchandises a poussé la création des Accords de Schengen de 1985[15]. En effet, au regard des formalités bien trop lourdes et des contrôles aux frontières trop long à la frontière franco-allemande, les transporteurs routiers ont fait grève pour manifester leur mécontentement. Leurs doléances ont été entendues par la signature de l'Accord de Sarrebruck[16], le 13 juillet 1984, qui prévoit la suppression des frontières entre l'Allemagne et la France. En parallèle, la Belgique, les Pays-Bas et le Luxembourg, qui forment le Benelux, ont décidé d'instituer une union économique et un espace sans contrôles à leurs frontières, le 03 février 1958[17].

Dans cette volonté d'abolir leurs frontières communes, ces cinq Etats ont décidé en 1985 de signer l'Accord de Schengen. Ce texte fondamental affirme le principe de liberté de circulation des personnes et prévoit par conséquent l'abolition totale des contrôles aux frontières de ces Etats. C'est ainsi que naît la notion de frontières extérieures. Cependant, en 1985, l'Accord de Schengen ne prévoit que les principes de l'espace Schengen. En effet, il faudra attendre 1990 pour que la Convention d'application de Schengen[18] vienne donner en détail les conditions de ce régime juridique. Tous les Etats signataires mettent un terme aux contrôles aux frontières à partir de 1995. L'espace Schengen met en place une coopération policière judiciaire et douanière, notamment grâce à l'instauration du Système d'information de Schengen ainsi qu'une politique commune de visa et d'asile.

La politique commune d'asile mise en par la Convention de Dublin[19] de 1990 ne sera pas abordée dans ce mémoire.

.

Dans les années 1980, la Communauté Economique Européenne doit faire face à de multiples crises qui l'empêchent de poursuivre la construction du marché intérieur. Face à ce constat, Jacques Delors, Président de la Commission européenne, publie le 14 juin 1985 le Livre blanc sur l'achèvement du marché intérieur. Ce texte préconise notamment *« l'élimination des frontières physiques, techniques et fiscales »*[20]. La réalisation de cette ambition est fixée pour le 31 décembre 1992, devenant ainsi « l'objectif 92 ». A cette

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

[16] Accord entre la France et la République fédérale d'Allemagne du 13 juillet 1984 relatif à la suppression graduelle des contrôles à la frontière franco-allemande

[17] Traité instituant l'Union économique Benelux du 03 février 1958

[18] Convention d'application de l'accord de Schengen du 14 juin 1985 du 19 juin 1990 entre les gouvernements des Etats de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes

[19] Convention de 1990 relative à la détermination de l'Etat responsable de l'examen d'une demande d'asile présentée dans l'un des Etats membres des Communautés européennes

[20] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:51985DC0310&from=FR

même période, les institutions européennes tentent de développer les notions de citoyenneté européenne et d'identité européenne, afin de créer une dynamique et retrouver une fédération entre les Etats membres.

L'année 1986, constitue également la naissance du marché intérieur de l'Union européenne grâce à l'Acte unique européen de 1986. Le principe de la liberté de circulation est désormais inscrit à l'article 3 du Traité sur le Fonctionnement de l'Union européenne (ci-après « TFUE ») et constitue une liberté fondamentale mais qui s'applique au-delà de l'espace Schengen puisqu'elle comprend la liberté de circulation des personnes, des marchandises, des services et des capitaux.

L'Espace de Liberté, de Sécurité et de Justice (ci-après « ELSJ ») était mentionné dans le Traité de Rome de 1957 mais prends véritablement sa substance en 1992 avec le Traité de Maastricht. Cet espace est désormais codifié dans le TFUE aux articles 67 à 89. Il a ainsi existé une interférence entre ces deux ordres juridiques. En effet, l'Union européenne ne doit pas être confondue avec l'espace Schengen. Alors que la première désigne l'organisation supranationale, le second est un espace de libre circulation des personnes. La mise en place de l'ELSJ est en revanche permise grâce à l'espace Schengen.

Il sera nécessaire d'attendre le Traité d'Amsterdam en 1997 pour que les accords de Schengen soient intégrés pleinement au droit primaire de l'Union européenne. A partir de cette date, chaque Etat candidat à l'intégration de l'Union européenne doit accepter les règles de Schengen. En effet, l'acquis Schengen devient un prérequis[21].

Aujourd'hui, l'espace Schengen compte 26 Etats dont 22 de l'Union européenne ainsi que la Norvège, l'Islande, la Suisse et le Liechtenstein. La Bulgarie, la Roumanie et la Croatie sont censés rejoindre prochainement cet espace mais diverses causes freinent cette intégration. Les territoires ultra-marins et la Guyane française n'appartiennent pas à l'espace Schengen.

[21] Cours de Droit européen des personnes, Mme SAULNIER-CASSIA Emmanuelle, année universitaire 2019-2010

III. La nécessité accrue d'obtention de documents permettant le voyage

Pour se déplacer en dehors de son pays, chaque individu doit être en possession d'une pièce d'identité et dans certains cas d'un visa. La pièce d'identité peut avoir plusieurs formes mais il est répandu de faire référence au passeport quand il s'agit de déplacements à l'étranger. Alors que le passeport est délivré par l'Etat dont l'individu est ressortissant, le visa est octroyé sur demande, par l'Etat de destination où le voyageur souhaite aller. Cette exigence ne date pas d'hier puisqu'elle est apparue dès le XVe siècle.

L'Encyclopédie définit ce document comme *« une permission accordée par une autorité souveraine à un individu ou un groupe d'individus afin d'entrer ou sortir de son territoire, librement et sans être inquiété »*.

Le passeport est la pièce d'identité la plus ancienne En effet, son apparition date à partir du XVe siècle. L'autorité souveraine signait des « passe-port » pour autoriser les voyageurs désirant quitter la France par la mer. Au nom de la liberté de circulation, la nécessité d'obtention de ce document est abrogée lors de la Révolution française. Mais dès 1792, le décret du 10 vendémiaire an IV instaure un « passeport pour l'intérieur » pour tous les citoyens français. Avec le développement du chemin de fer dans les années 1860 et la multiplication des déplacements, c'est la fin du passeport pour l'intérieur. Ce document fera son retour le 03 août 1914 au regard du contexte de la Première guerre mondiale. Une intensification des contrôles documentaires sera opérée lors de la Seconde guerre mondiale[22]. Il est intéressant d'observer, grâce à l'Histoire, le lien qui existe entre les régimes autoritaires et dictatoriaux (l'Italie fasciste, l'Afrique du Sud durant l'apartheid, l'Union soviétique) et l'obligation de détention de pièce d'identité afin d'exercer un réel contrôle sur le déplacement de leurs ressortissants.

L'article 12 du Pacte international relatif aux droits civils et politiques de 1966 autorise tout individu à entrer et à quitter librement son territoire. Cependant, l'entrée sur le territoire d'un étranger demeure de la souveraineté de l'Etat de destination.

L'apparition du visa, telle que connu aujourd'hui, date de la fin du XVIIIe siècle, avec la crainte d'une invasion venant du nord de la France. À la suite de l'attentat contre Napoléon III en 1858, l'empereur exige que tous les étrangers doivent détenir un livret tamponné par le Consul français. Une exception sera accordée en 1874 pour les ressortissants des pays frontaliers. Une ordonnance du 02 novembre 1945[23] prévoit le visa

[22] https://www.lozere.gouv.fr/Laissez-passer-les-p-tits-papiers-petite-histoire-du-passeport
[23] Ordonnance n°45-2658 du 02 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France

comme document nécessaire afin d'entrer sur le territoire français. Des exceptions commencent alors à être accordées aux ressortissants de Nouvelle-Zélande en 1947 ou encore aux ressortissants américains en 1949. En 1957, le Conseil de l'Europe signe un accord européen sur le régime de la circulation des personnes dans lequel il est décidé d'accorder des dispenses s'il existe des réciprocités avec l'Etat partenaire pour des séjours ne devant dépasser un délai de trois mois maximum[24].

Après la naissance de l'aviation commerciale, le 01e janvier 1914[25], il a été nécessaire d'uniformiser les prérequis en termes de documents de voyage nécessaires quand le transport s'effectue par un aéronef. L'annexe 9 de 1944 de l'Organisation de l'aviation civile internationale (ci-après « OACI ») est relative à la facilitation. Son chapitre 3 prévoit les standards applicables à l'entrée et à la sortie des personnes et de leur bagage. Quand le transport s'effectue par voie aérienne, les Etats ne peuvent exiger d'autres documents que le passeport et un visa. Aucun Etat signataire ne peut enjoindre les étrangers d'obtenir un visa de sortie ni de visa de retour pour ses ressortissants. Chaque Etat est investi de prérogative d'inspection des documents de voyage. Une aide doit également être apportée aux transporteurs aériens dans cette mission qui demeure régalienne. Des pratiques sont également recommandées en ce qui concerne la sécurité de ces documents pour éviter la fraude.

Les attentats du 11 septembre 2001 marquent un tournant capital dans la sureté aérienne et notamment dans la vérification documentaire. La sureté ne doit pas être confondue avec la sécurité. Alors que la première tente d'éviter tout acte malveillant, la sécurité est relative aux risques pouvant survenir accidentellement ou par négligence, sans aucune intention de son auteur. Les règles liées à la sureté aérienne sont codifiées par l'Annexe 17 de l'OACI. La prise de conscience d'une nouvelle menace que constitue le terrorisme a poussé les Etats à se doter de technologies de plus en plus sures, tels que les passeports biométriques, et d'accroitre la surveillance sur les déplacements des individus en recourant à des systèmes d'information de plus en plus performants et détaillés.

[24] Accord européen sur le régime de circulation des personnes entre les pays membres du Conseil de l'Europe, 13 décembre 1957

[25]https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20131227trib000802909/il-y-a-100-ans-naissait-l-aviation-commerciale-et-ca-coutait-cher.html

IV. La conciliation entre protection des données et la sûreté des frontières

Au regard des défis qui s'imposent face à aux menaces terroristes mais également sanitaires, telle qu'en témoigne la pandémie de la Covid-19, les Etats doivent veiller à la sécurité de leurs frontières. Alors que cette mission régalienne est déjà un enjeu pour un seul Etat, ce challenge devient plus laborieux quand un espace sans contrôles aux frontières intérieures est instauré, tel que l'espace Schengen. Les Etats membres ont accepté, au nom de l'intégration européenne, de transférer une partie de leur souveraineté à l'Union européenne. Or, aujourd'hui, au regard de l'ampleur de la tâche, des tensions se cristallisent et des remises en question s'opèrent allant jusqu'à la montée d'un euroscepticisme exacerbé par certains partis politiques.

Désireux d'accroître la sûreté et la sécurité de l'espace Schengen et donc de veiller à un contrôle rigoureux des frontières extérieures, l'Union européenne a décidé de mettre en place, dès mai 2022, une autorisation électronique de voyage, appelée ETIAS *(European Travel Information and Autorisation System)*, pour les ressortissants non soumis à l'obligation de visa. Cela représente 20% des étrangers entrant sur le territoire de l'espace Schengen. L'ETIAS a cette ambition d'élever le niveau de sécurité et de sûreté. En effet, elle a pour objectif d'évaluer le risque que pourrait constituer un migrant vis-à-vis de l'ordre public mais également de prévenir les risques sanitaires. Cependant, ce nouveau système opère une collecte grandissante des données à caractère personnel au nom de la sécurité publique.

Or, l'Union européenne s'est illustrée ces dernières années avec l'adoption du Règlement Général de Protection des Données (ci-après « RGPD), le 27 avril 2016. Ce texte permet un niveau élevé de protection des données personnelles et accorde également des droits hautement protecteurs pour les individus concernés. Une donnée à caractère personnelle peut être définie comme étant « *toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une personne physique identifiable une personne physique qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant, tels qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »[26].

[26] Article 4 paragraphe 1 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

L’instauration de cette autorisation de voyage peut poser question sur une remise en cause du RGPD, sur la conciliation des principes découlant de ce texte et les défis auxquels les Etats doivent faire face pour assurer des niveaux de sûreté et de sécurité élevés. La protection et la sécurité peuvent-elles être conciliables ou bien la pratique démontre-t-elle la nécessité de faire un choix ?

En somme, le droit à la protection des données à caractère personnel est-il pleinement effectif face aux enjeux de la sureté et de la sécurité des frontières extérieures de l’espace Schengen à l’image de la mise en place de l’ETIAS ?

Pour y répondre, il est nécessaire de s’interroger sur les défis de la sûreté et de la sécurité des frontières extérieures de l’espace Schengen qu’il est aujourd’hui nécessaire de surmonter (I) afin d’apprécier les enjeux du droit à la protection des données à caractères personnel face à ces nouveaux besoins (II).

Partie I – LES DÉFIS DE LA SÛRETÉ ET DE LA SÉCURITÉ DES FRONTIÈRES EXTÉRIEURES EN EUROPE À SURMONTER

La mise en place d'un système électronique d'autorisation de voyage tel que l'ETIAS (I) contribue à la création de systèmes d'information qui collectent un nombre grandissant de données à caractère personnel (II).

Titre I - La nécessité d'un système électronique d'autorisation de voyage

La remise en cause du système actuel de l'espace Schengen (I) a pour conséquence la création d'un système électronique d'autorisation de voyage qui s'accompagne nécessairement de mutations importantes (II).

Chapitre I. La remise en cause du système actuel de l'espace Schengen

Ces dernières années ont permis d'observer que les principes fondamentaux des accords de Schengen (I) ont subi de fortes critiques induisant indubitablement une réforme en 2021 (II).

Section I. Les principes fondamentaux des accords de Schengen

Les accords de Schengen prévoient la suppression des contrôles aux frontières intérieures au profit d'un renforcement aux frontières extérieures (I), une politique commune de visas de court séjour (II) ainsi que l'établissement et le développement du Système d'Information Schengen (III).

I. La disparité des frontières intérieures pour un renforcement des frontières extérieures

1.-Principe – Aboutissement de la construction du marché intérieur, l'article 2§1 de la Convention de Schengen du 14 juin 1985 et l'article 67§2 du Traité sur le fonctionnement de l'Union européenne prévoient la suppression de tous les contrôles de personnes aux frontières intérieures. Ainsi, toute personne peut circuler librement à l'intérieur de l'espace Schengen. Cependant, cette abolition nécessite une contrepartie, qu'est le renforcement des frontières extérieures, c'est-à-dire entre les Etats membres et les Etats tiers. Des règles communes sont érigées par le Règlement 562/2006 du 15 mars 2006[27],

[27] Règlement n° n° 562/2006 du 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes

qui créé le code communautaire relatif au régime de franchissement des frontières par les personnes, appelé Code frontières Schengen. Ce Règlement, qui abroge les articles 2 à 8 de la Convention de Schengen, a été modifié par le Règlement 2016/344 du 09 mars 2016[28]. Le considérant 6 dudit Règlement prône la solidarité entre les Etats membres en ce qui concerne les contrôles des frontières : *« le contrôle aux frontières n'existe pas seulement dans l'intérêt de l'Etat membre aux frontières extérieures duquel il s'exerce, mais dans l'intérêt de l'ensemble des Etats membres ayant aboli le contrôle aux frontières à leurs frontières intérieures ».* Ainsi, la surveillance des frontières, et ce en particulier pour les Etats qui possèdent des frontières extérieures, doit se réaliser en concert et induit nécessairement une responsabilité envers tous les autres Etats membres. L'ambition des traités est que chaque Etat accepte de rogner sur ses prérogatives de puissance publique à la seule condition que les autres Etats veillent scrupuleusement à leurs frontières. Une distinction est donc faite entre le franchissement des frontières extérieures et le franchissement des frontières intérieures, respectivement prévus par les titres II et III du Code frontières Schengen. Toutefois, cette abolition des frontières intérieures n'interdit pas tout contrôle de la part des Etats membres. En effet, l'article 21 prévoit la possibilité pour les autorités de procéder à des contrôles pour des motifs d'ordre public y compris sur les zones frontalières.

2.-Exception – Voulant garder une main mise sur leur souveraineté, les Etats membres originels ont négocié, lors de l'élaboration des accords Schengen, une clause de sauvegarde prévue par l'article 2§2 de la Convention et aux articles 23 à 35 du Code frontières Schengen. Les Etats membres peuvent rétablir temporairement leurs contrôles aux frontières intérieures si l'ordre public ou la sécurité nationale l'exigent. Tel fût le cas lors de la Coupe du monde de football en Allemagne en 2006 ou encore lors des sommets du G8. Cependant, le Code frontières Schengen indique explicitement que cette exception à la libre circulation des personnes ne peut être mise en place *« qu'en dernier recours »,* et ce *« pendant une période limitée d'une durée maximale de trente jours ou pour la durée prévisible de la menace grave si elle est supérieure à trente jours* ». La Cour de Justice de l'Union Européenne (ci-après « CJUE ») exerce un contrôle et exige qu'une menace réelle et suffisamment grave touche l'intérêt fondamental de l'Etat[29]. Ainsi, l'ambition des traités est que cette clause de sauvegarde, qui constitue un garde-fou, ne puisse être appliquée que pour un court délai et de façon exceptionnelle grâce à des conditions strictes de mise en œuvre. La procédure nécessite que les autres Etats membres et la Commission européenne soient informés en amont, sauf en cas d'urgence où une simple

[28] Règlement n° 2016/399 du 09 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes

[29] CJCE, 1e chambre, Nural Ziebell c/ Land Baden-Württemberg, 08 décembre 2011, n°371/08

notification sera suffisante. Il est important de souligner que les textes originels ne prévoient en aucun cas la possibilité pour les Etats membres de réintroduire les contrôles aux frontières intérieures en cas de défaillance d'un autre Etat à ses obligations.

II. La distinction entre les ressortissants de pays tiers soumis à visa et ceux exemptés

3.- Différenciation en fonction du risque migratoire – L'article 9 de la Convention de Schengen a imposé aux Etats contractants d'avoir une politique commune en matière de visas, à des fins d'harmonisation. Les Etats ont alors fait une distinction entre les ressortissants de pays tiers soumis à l'obligation de visa et ceux qui en étaient dispensés. Le Règlement 539/2001 du 15 mars 2001[30] qui dresse la liste des pays tiers a été modifié à plusieurs reprises en augmentant le nombre d'Etats dont les ressortissants sont soumis à cette obligation préalable. Aujourd'hui, 44 Etats inscrits à l'annexe 2 bénéficient de la possibilité pour leurs ressortissants d'entrer dans l'espace Schengen sans aucune formalité particulière au préalable. Cette liste a un caractère juridique contraignant et l'Etat qui souhaite y déroger doit *« consulter les autres Parties contractantes et dans sa décision, tenir compte de leurs intérêts ainsi que des conséquences de cette décision* ». Cette disposition fait référence au principe de solidarité que doivent respecter les Etats. Cette distinction s'explique par le fait que les Etats membres considèrent que les Etats exemptés ont un faible risque migratoire et de santé publique. En 2017, l'Union européenne a délivré 16,1 millions de visa de court séjour et la France près de 3,6 millions, ce qui en fait le premier Etat membre à délivrer des visas Schengen[31]. Le code des visas institué par le Règlement 910/2009 prévoit les conditions et les procédures pour l'octroi des visas de court séjour ainsi que les visas de transit aéroportuaire[32]. Il existe trois types de titre de séjour : le visa Schengen uniforme, le visa à validité territoriale limitée et les visas nationaux.

4.- Visa Schengen Uniforme – Le visa Schengen Uniforme s'applique aux visas de catégories A et C et est valable dans tout l'espace Schengen. Le visa de transit aéroportuaire, de catégorie A, est obligatoire en cas de voyage entre deux Etats n'appartenant pas à l'espace Schengen en passant par un Etat Schengen. Il est considéré que le passager reste dans la zone internationale de l'aéroport sans toutefois entrer dans l'espace Schengen. Quant au visa de séjour de courte durée, de catégorie C, il peut être

[30] Règlement (CE) n° 539/2001 du Conseil du 15 mars 2001 fixant la liste des pays tiers dont les ressortissants sont soumis à l'obligation de visa pour franchir les frontières extérieures des Etats membres et la liste de ceux dont les ressortissants sont exemptés de cette obligation

[31] Rapport d'information n°898 de l'Assemblée nationale sur l'Espace Schengen et la maîtrise des frontières extérieures de l'Union européenne produit par Messieurs les Députés Ludovic MENDES et Christophe NAEGELEN

[32] Règlement (CE) n°810/2009 du 13 juillet 2009 établissant un code des visas pour l'Union européenne

obtenu sous plusieurs formes : entrée unique, double entrée ou entrées multiples. Il permet à tout étranger qui le possède d'effectuer un séjour de 90 jours maximum sur une période de 180 jours. La demande, qui est faite en ambassade ou au consulat de l'un des Etats Schengen, doit être effectuée auprès de l'Etat membre qui est la destination principale de l'étranger, à défaut c'est l'Etat de la première entrée dans l'espace Schengen. L'autorité chargée de l'étude du dossier doit vérifier si les conditions établies par le Code frontières Schengen et le Code des visas sont remplies. Un demandeur peut voir sa demande refusée s'il constitue une menace pour l'ordre public, s'il ne fournit pas les preuves qu'il dispose de ressources suffisantes pour séjourner et revenir dans son Etat d'origine, ou encore s'il fournit de fausses informations ou de faux documents. La décision de délivrance ou de refus doit être respectée par tous les Etats parties. Ainsi en cas de refus, un Etat doit empêcher l'individu de se rendre dans n'importe quel autre Etat partie. En outre, l'Etat qui délivre un titre de séjour est considéré comme étant responsable de l'entrée du ressortissant d'un pays tiers. Ainsi, si ce dernier se rend dans l'espace Schengen dans des conditions irrégulières, alors en vertu des accords de réadmission prévus par l'article 23 de la Convention de Schengen, l'Etat responsable devra reconduire l'individu dans son pays d'origine ou vers l'Etat d'origine. Des accords de facilitation, permettant la simplification de la délivrance de visas, ont été signés avec la Chine, le Maroc ou encore la Biélorussie. Les non-ressortissants de l'Union européenne ont une obligation de déclaration s'ils quittent le territoire d'un Etat Schengen pour entrer dans un autre. Cette politique commune de visa possède une exception pour les membres de la famille[33] d'un ressortissant de l'Union européenne. En effet, en vertu de l'article 5.2 de la Directive 2004/38/CE[34], ces non ressortissants de l'Union européenne peuvent soit demander un visa soit, s'ils en font la demande, obtenir de plein droit une carte de séjour dénommé « Carte de séjour de membre de la famille d'un citoyen de l'Union ». Cette Directive vise au regroupement familial.

5.- Visa à validité territoriale limitée – Le visa à validité territoriale limitée permet d'être admis uniquement dans l'un des Etats de l'espace Schengen. Ce type de visa n'est délivré que pour des raisons humanitaires ou sur motif d'intérêt national.

6.- Visas nationaux – La Convention de Schengen et le Code de visa ne créent pas de visa Schengen pour les séjours de longue durée, c'est-à-dire de plus de trois mois. Ainsi, chaque Etat délivre un visa selon sa propre législation. Il permet aux ressortissants de pays tiers d'étudier, de travailler ou résider de manière permanente.

[33] Désigne, d'après l'article 2, le conjoint, le partenaire de PACS, les descendants directs âgés de moins de vingt-et-un an et ceux du conjoint ou partenaire, les ascendants directs et ceux du conjoint ou du partenaire

[34] Directive 2004/38/CE du 29 avril 2009 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des Etats membres

III. L'établissement et le développement du Système d'Information Schengen

7.- Objectifs – Entré en service en 1995, le Système d'Information Schengen (ci-après « SIS ») est une base de données d'informations partagées entre les pays de l'espace Schengen et de l'Union européenne et est géré par la Commission européenne. Son objectif est d'assurer un niveau élevé de sécurité dans l'Espace de Liberté Sécurité et de Justice de l'Union grâce à une coopération policière, des contrôles frontaliers et d'immatriculation des véhicules. Cette base de données permet d'introduire ou de consulter des signalements concernant des personnes, des objets recherchés ou portés disparus. Le SIS fournit toutes les informations sur la conduite à tenir face à l'individu ou l'objet. Les signalements peuvent être divers : des individus qui font l'objet d'un mandat d'arrêt ou qui se sont vu refuser l'accès à l'espace Schengen, des objets volés ou qui constituent des preuves dans des procès, des alertes préventives pour des personnes vulnérables qui risquent d'être enlevées. En cas d'alerte, les autorités peuvent arrêter l'individu, saisir l'objet ou encore procéder à des contrôles. Ces signalements émanent à la fois de bases de données nationales et du SIS. Chaque Etat dispose d'un bureau SIRENE qui constitue le point de contact national. Ils ont pour mission de fournir toutes les informations supplémentaires sur les signalements émis et sont chargés de coordonner les activités menées[35].

8.- Champ d'application – 27 Etats utilisent aujourd'hui le SIS. Cependant, son champ d'application territorial varie car tous ces pays n'utilisent pas pleinement le SIS. En effet, la Croatie ne coopère qu'en matière policière et ne peut introduire de signalement. Il en est de même pour l'Irlande, la Bulgarie et la Roumanie. Des travaux préparatoires sont actuellement en cours pour que Chypre et la Croatie puissent intégrer pleinement le SIS. Avant le Brexit, le Royaume-Uni n'appliquait le SIS que de manière partielle dans le cadre de la coopération policière. Cette application partielle a pour principal inconvénient d'amoindrir la portée de cette base de données. En effet, seule une véritable coopération d'un maximum de pays permettrait au SIS d'atteindre au mieux son objectif.

9.- Des difficultés de mise en œuvre du SIS II – Dès 1996, les pays membres de l'espace Schengen ont décidé de développer le SIS II. Mais celui-ci n'est entré en vigueur que le

[35] Mémoire de Catherine MSELLATI, « La Convention d'application de l'accord de Schengen et ses implications en matière de transport aérien », Octobre 1996

09 avril 2013 par les Règlements 1986/2006[36] et 1987/2006[37] ainsi que la décision[38] du Conseil du 12 juin 2007. Malgré une date butoir d'achèvement fixée à décembre 2006 par le Conseil, cette base de données a été opérationnelle six ans plus tard et avec un dépassement de budget colossal (de 23 à 189 milliards d'euros)[39]. Ces difficultés s'expliquent par un projet au départ trop ambitieux, peu d'agents disposant des compétences nécessaires, une mésentente importante entre certains pays membres et la Commission européenne et des essais opérationnels infructueux[40]. Une mutation importante a donc eu lieu en 2013 lors de la mise en service du SIS II. En effet, de nouvelles catégories de signalements d'objets ont été rajoutées, tels que les aéronefs, le recours aux données biométriques pour confirmer l'identité d'un individu ou encore l'ajout de données complémentaires pour détecter les usurpations d'identité. En 2019, avec 91 millions[41] de signalements recensés dans le SIS II, la Commission européenne considère que cette base de données est un succès permettant de lutter efficacement contre la criminalité : *« le SIS II apporte une réelle valeur ajoutée européenne (…) Aucun autre système de coopération policière ne génère autant de résultats positifs ni n'est en mesure de traiter en temps réel un tel flux d'informations, et en conséquence le nombre de réponses positives dans toutes les catégories de signalements augmente d'année en année »*[42].

10.- Données collectées – La portée et les fonctionnalités du SIS ayant été élargies, de plus en plus de données sont collectées afin d'alimenter cette base de données. Tout individu est susceptible d'être sur cette base de données, et ce sans distinction de nationalité. Il n'est pas informé de son inscription au fichier sauf si celle-ci résulte d'une décision de refus de délivrance de visa. En outre, la personne signalée ne peut s'opposer à cette inscription car il est considéré que le SIS concerne la sécurité de l'Etat, la défense de la sécurité publique. Cependant, des conditions strictes sont mises en place. En effet, les Etats doivent justifier l'accès d'une autorité aux données qui figurent dans le fichier. Il est intéressant de noter que le nombre de ces autorités augmente au fil du temps. Originellement, la police, les services douaniers, agents d'immigration et visa, Europol

[36] Règlement (CE) n°1986/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'accès des services des Etats membres chargés de l'immatriculation des véhicules au Système d'Information Schengen de deuxième génération

[37] Règlement (CE) n°1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du Système d'Information Schengen de deuxième génération

[38] Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du Système d'Information Schengen de deuxième génération

[39] Rapport spécial de 2014 de la Cour des Comptes Européenne – « Les enseignements tirés du développement par la Commission du système d'information Schengen de deuxième génération »

[40] Rapport spécial de 2014 de la Cour des Comptes Européenne – « Les enseignements tirés du développement par la Commission du système d'information Schengen de deuxième génération »

[41] https://www.cnil.fr/fr/sis-ii-systeme-dinformation-schengen-ii

[42] Rapport de la Commission du 21 décembre 2016 sur l'évaluation du Système d'Information Schengen de deuxième génération

ou encore l'autorité d'immatriculation des véhicules ont accès au SIS. Lors de la réforme, cette liste a été étendue aux autorités d'immatriculation de navires et d'aéronefs ainsi qu'à Frontex.

Section II. Les difficultés de Schengen imposant la réforme en 2021

L'espace Schengen connaît aujourd'hui des difficultés suscitant sa contestation notamment au regard du contrôle des frontières extérieures (I), c'est la raison pour laquelle une réforme s'impose aujourd'hui (II).

I. La problématique du contrôle des frontières extérieures

La problématique du contrôle des frontières extérieures est en partie causée par un manque flagrant de coordination et de confiance entre les Etats membres (A), et ce malgré les efforts importants des institutions de l'Union européenne, pourtant jugés insuffisants (B).

A. Le manque de coordination et de confiance mutuelle

11.- Des crises poussant les Etats à détourner la clause de sauvegarde – La crise migratoire découlant du Printemps arabe en 2011, puis les différentes attaques terroristes de 2015 et plus récemment la pandémie de la Covid-19 ont révélé les lacunes et les tensions existantes. En effet, à chacune de ces crises, les Etats membres ont tous eu un seul et même réflexe : se retrancher derrière leurs frontières respectives. La France, l'Allemagne, l'Autriche, la Suède, le Danemark et la Norvège sont les Etats qui ont rétabli des contrôles à leurs frontières intérieures[43], et ce depuis 2015 alors que la clause de sauvegarde affirme de manière explicite le caractère temporaire et extraordinaire de cette entrave à la libre circulation. Or, la clé de voute de l'espace Schengen est la solidarité, financière et opérationnelle, mais également la confiance mutuelle, au regard des contrôles opérés à l'entrée sur l'espace commun. Yves Bertoncini, Président de l'Institut Jacques Delors, pointe clairement la problématique *« Il y a derrière tout ça un problème de confiance mutuelle : certains Etats membres n'ont pas confiance dans la capacité d'autres Etats membres à contrôler nos frontières extérieures »*[44], bien que la CJUE considère que la confiance mutuelle est un « principe d'importance fondamentale »[45]. Cependant, ce principe n'étant assorti d'aucune contrainte juridique, il ne peut exister que

[43] Cartographie Le Monde de Francesca Fattori et Xemartin Laborde
[44] https://www.rfi.fr/fr/emission/20151216-union-europeenne-vers-super-frontex-pouvoirs-migration-schengen
[45] CJUE, avis 2/13 du 18 décembre 2014, point 191

selon le bon vouloir des Etats[46]. Après ces constatations, il est important de comprendre les causes induisant cette méfiance à l'égard des autres partenaires du traité.

12.- Le mécanisme d'évaluation et de contrôle de Schengen – L'espace Schengen dispose d'un mécanisme d'évaluation et de contrôle, qui a fait l'objet d'une profonde réforme en 2013 : le Règlement SCH-EVAL[47]. Dans le cadre d'une responsabilité partagée, la Commission européenne effectue les évaluations avec des experts des Etats membres, puis le Conseil formule des recommandations sur la base d'une proposition de la Commission afin de remédier aux manquements constatés. Chaque Etat connaît au moins une évaluation tous les cinq ans mais il est possible d'avoir des contrôles inopinés. Les Etats sont dans l'obligation de présenter à la Commission des mesures correctives et de rendre compte de l'avancement des actions entreprises. Si la Commission constate que les manquements constatés n'ont pas été solutionnés, alors une réintroduction des contrôles aux frontières intérieures peut avoir lieu. Le premier programme d'évaluation, ayant eu lieu entre 2015 et 2019, permet d'obtenir des éléments de compréhension. En effet le rapport de la Commission[48], dressé en 2020, indique que bien que l'ensemble des *« Etats membres respectent les dispositions essentielles de l'acquis de Schengen dans tous les domaines d'action »,* des pratiques divergentes entre les Etats membres sont constatées, ce qui a pour conséquence d'affaiblir de manière significative les règles fixées. En effet les contrôles aux frontières varient d'un pays à l'autre en raison de difficultés liées à la formation ou l'effectif. Le rapport dénonce également le « visa shopping » employé par le personnel consulaire qui considèrent les visas Schengen tels que des visas nationaux. Une divergence importante existe en ce qui concerne la détermination de la validité des visas et des pièces justificatives à exiger ou encore sur la qualité des données saisies dans le SIS. Dans tous les domaines évalués le manque de ressources tant humaines que financières est souligné. Or ces ressources proviennent de la volonté des Etats membres.

13.- La fragilisation de l'espace Schengen causée par les Etats membres - Toutes ces faiblesses, qui émanent des Etats membres eux-mêmes, créent des problématiques liées aux contrôles des frontières extérieures induisant nécessairement une méfiance et un repli sur soi, ce qui fragilise l'existence même de l'espace Schengen. Au-delà de celle-ci, les Etats vont jusqu'à déconstruire des principes fondamentaux de l'espace Schengen. La crise franco-italienne en est un exemple. En effet, submergé par l'immigration clandestine en janvier 2011, le Président du Conseil italien, Silvio Berlusconi réclame de l'aide à ses

[46] H. Labayle « Schengen, un espace dans l'impasse », *Revue Europe,* Mars 2016
[47] Règlement (UE) n°1053/2013 du Conseil du 07 octobre 2013 portant création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen
[48] Rapport de la Commission au Conseil et au Parlement européen du 25 novembre 2020 sur le fonctionnement du mécanisme d'évaluation et de contrôle de Schengen

partenaires européens qui n'accèdent pas à cette demande, jugeant l'afflux de migrants trop modeste. En vertu de l'article 20 du décret législatif n°29 du 25 juillet 1998, l'Italie décide le 05 avril 2011 d'accorder des titres de séjour, pour des raisons humanitaires, aux migrants pour circuler librement dans l'espace Schengen. Trois jours plus tard, Claude Guéant, Ministre de l'Intérieur français, rétablit temporairement le contrôle à la frontière franco-italienne. Devant cette situation, le 26 avril 2011, Silvio Berlusconi et Nicolas Sarkozy, Président de la République Française, adressent une lettre[49] au Président du Conseil européen, Herman Van Rompuy et au Président de la Commission européenne, José Manuel Barroso afin que soit autorisé *« le rétablissement temporaire des contrôles aux frontières intérieures en cas de difficultés exceptionnelles dans la gestion des frontières extérieures »*. C'est ainsi que Yves Pascouau affirme que *« l'avenir de l'Espace Schengen ne se décide pas à Bruxelles mais dans chaque Etat membre »*[50]. L'Union européenne ne serait-elle pas un coupable idéal alors que l'arsenal déjà existant n'est pas appliqué rigoureusement par les Etats ou bien celui-ci est-il réellement insuffisant légitimant ainsi les nombreuses polémiques autour du contrôle des frontières extérieures ?

14.- Le cas de la France – La France a aussi fait l'objet d'une évaluation mettant en évidence 18 points de non-conformité qui concernent essentiellement les ressources, la formation et l'organisation du travail. Les aéroports de Paris-Orly et Nice-Côte d'Azur sont régulièrement mentionnés, notamment sur la qualité du contrôle frontière. Un plan de formation est prévu par la police aux frontières concernant la réglementation et l'utilisation des différents outils existants afin de remédier aux lacunes constatées.

B. Les efforts importants de l'Union européenne mais insuffisants

15.- La concession sur la durée des contrôles aux frontières intérieures - Lors d'une réunion du Conseil Justice et affaires intérieures, cinq Etats ont souhaité modifier l'article 25 et 27 du Code Schengen en permettant un rétablissement temporaire des contrôles aux frontières intérieures pendant deux ans, voire quatre ans en cas de menace grave. Afin d'apaiser les tensions politiques et la montée de l'euroscepticisme, le 27 septembre 2017, la Commission accepte une prolongation des durées des contrôles aux frontières mais en contrepartie durcit les conditions[51]. Cette contrepartie est à nuancer car il est désormais exigé que cette entrave à la liberté de circulation puisse avoir lieu qu'en cas « de nécessité de réagir à l'évolution et à la pertinence de menaces grave ». Cette condition peut sembler bien trop large et trop floue ce qui permet d'avoir une appréciation extensive de la part

[49] https://www.vie-publique.fr/discours/181940-lettre-de-mm-nicolas-sarkozy-president-de-la-republique-et-silvio-ber
[50] Y. PASCOUAU, Question d'Europe n°392 du 17 mai 2016, Fondation Robert Schuman
[51] https://www.vie-publique.fr/en-bref/19728-schengen-la-commission-propose-une-modification-du-code-frontieres

de l'Etat qui souhaite rétablir ses contrôles. La procédure est également revue à cette occasion.

16.- Des vérifications systématiques pour tous – Aux frontières, tant intérieures qu'extérieures, une distinction est faite entre les citoyens de l'Union européenne, les membres de leur famille et les ressortissants de pays tiers[52]. Les citoyens de l'Union européenne ainsi que les membres de leur famille sont soumis aux dispositions de l'article 20§1 du TFUE et à la Directive 2004/38 où est posé un principe de vérification minimale qui est repris par l'article 8 du Code frontières Schengen. Les ressortissants de pays tiers sont eux soumis à une vérification approfondie, c'est-à-dire qu'une consultation des bases de données est systématiquement faite pour s'assurer que l'individu ne représente pas une menace pour l'ordre public ou la santé publique. Cependant, depuis avril 2017[53], cette vérification approfondie a également été élargie aux citoyens de l'Union européenne et aux membres de leur famille. Ces vérifications sont réalisées tant à l'entrée qu'à la sortie de l'espace Schengen. Cette extension répond au besoin d'accroitre les contrôles au regard des menaces terroristes bien plus importantes aujourd'hui et qui peuvent provenir des ressortissants de pays tiers mais également des ressortissants européens. Une dérogation de six mois existe uniquement pour les citoyens de l'Union européenne s'il s'avère que les vérifications ont un effet disproportionné sur la fluidité du trafic.

17.- Réforme sur les visas de courte durée – Dans l'optique d'assurer un haut niveau de sécurité au sein de l'espace Schengen, une importante réforme a été effectuée sur le Code communautaire des visas, devenu Code des visas Schengen, qui est entré en vigueur le 02 février 2020 par le Règlement 2019/1155[54]. Cette réforme a trois principaux axes. La première est la facilitation de la procédure d'obtention de visa par l'extension des périodes de dépôt des demandes qui peuvent être faites électroniquement, l'obligation de chaque Etat membre d'être présent sur le territoire de ses partenaires européens ou encore par la facilitation de l'obtention de visas pour les individus qui viennent régulièrement dans l'espace Schengen. Cette meilleure acceptabilité est cependant conditionnée par une attention accrue qui est portée sur l'assurance voyage, obligatoire pour tous les demandeurs, qui couvre notamment les frais médicaux éventuels. Enfin, un rapport de confiance est installé avec les pays tiers relatif à la réadmission des immigrants qui ne sont pas en conformité avec les règlementations en vigueur en ce qui concerne l'entrée

[52] C. DIRE, « Le concept de gestion intégrée des frontières », *Revue de l'Union européenne*, p.475
[53] Règlement (UE) n° 2017/458 du Parlement Européenne et du Conseil du 15 mars 2017 modifiant le Règlement (UE) n° 2016/299 en ce qui concerne le renforcement des vérifications dans les bases de données pertinentes aux frontières extérieures
[54] Règlement (UE) n° 2019/155 du Parlement européen et du Conseil du 20 juin 2019 portant modification du Règlement (CE) n° 810/2009 établissant un code communautaire des visas

sur le territoire de l'espace Schengen. En effet, plus un pays tiers coopèrera, plus la procédure d'obtention de visa pourra être facilitée[55].

18.- Fonds pour la sécurité intérieure – La géographie crée indubitablement des inégalités puisque tous les Etats membres de l'espace Schengen n'ont pas de frontières extérieures. Par conséquent, ces pays sont moins exposés aux flux de trafic frontalier. Ainsi, quatre fonds européens de solidarité ont été créés dont le fond pour la sécurité intérieure (FSI)[56]. Entre 2014 et 2020, ce fond a permis d'aider les autorités de ces Etats dans la gestion de leurs frontières extérieures, à hauteur de 2,8 milliards d'euros.

19.- Les conséquences en cas de sortie des accords de Schengen – L'Union européenne a mis en place plusieurs mesures, afin d'apaiser la montée grandissante de l'euroscepticisme et les polémiques concernant son incapacité à gérer les frontières extérieures, en acceptant plusieurs concessions et réformes. Cependant, il semblerait que les efforts entrepris ces dernières années ne sont pas suffisants. Certains dirigeants en viennent jusqu'à la menace de quitter ou suspendre les accords de Schengen, tel que Nicolas Sarkozy en 2014. Ce chantage, qui s'avère être davantage une pression politique, est à relativiser car les conséquences principalement économiques sont colossales. L'abandon des accords de Schengen, en ce qui concerne la France, représenterait une perte de dix milliards d'euros par an[57]. En plus d'une baisse des recettes touristiques (entre 500 millions et 1 milliard d'euros par an), un impact important sur le travail frontalier (150 millions d'euros), les flux de marchandises (130 millions d'euros) ou encore les investissements étrangers et flux financiers. Ces répercussions ne peuvent s'envisager que difficilement. Ainsi, à défaut de quitter les accords Schengen, les Etats membres n'ont que pour unique choix de trouver des solutions en passant par une profonde réforme afin de sauver l'acquis Schengen.

C. La réforme visant au sauvetage de l'acquis Schengen

Afin d'apaiser toutes les critiques, la France pousse les institutions européennes à mener une réforme (1) qui permettrait à l'espace Schengen d'être plus résilient. Ce vœu a été entendu puisque la « Stratégie Schengen » annoncée pour 2021 a pour ambition de sauver l'acquis Schengen (2).

---

[55] https://www.schengenvisainfo.com/fr/actualites/les-regles-du-visa-schengen-vont-changer-a-partir-de-fevrier-2020/
[56] https://www.europarl.europa.eu/factsheets/fr/sheet/153/gestion-des-frontieres-exterieures
[57] Note d'analyse, « Les conséquences économiques d'un abandon des accords de Schengen », *France Stratégie*, Février 2016, N°39

1. La France à l'initiative de cette réforme

20.- Les propositions formulées – Lors des élections européennes, en mars 2019, Emmanuel Macron, Président de la République Française, tente une première initiative dans une lettre adressée aux Français, dans laquelle il propose « une remise à plat » de Schengen. Mais c'est lors de son déplacement à Perthus, le 05 novembre 2020 qu'il s'exprime davantage sur le contrôle aux frontières : *« je suis favorable à ce que nous refondions en profondeur Schengen pour en repenser l'organisation, pour intensifier notre protection commune aux frontières avec une véritable police de sécurité aux frontières extérieures de l'espace, en renforçant aussi l'intégration de nos règles et en réussissant à construire aussi un fonctionnement conjoint de nos ministres en charge justement de l'Intérieur et de la Sécurité pour que l'Europe fonctionne de manière beaucoup plus intégrés sur ce sujet »*[58]. Il promet à cette occasion de doubler les effectifs français aux frontières et ainsi de passer de 2 400 agents à 4 800. Sous pression également du parti d'extrême droite dans son pays, Sébastien Kurz, Chancelier fédéral d'Autriche décide de soutenir son homologue français lors d'une conférence de presse conjointe tenue le 10 novembre dernier dans laquelle ils s'expriment sur leur souhait de *« mettre en place un véritable Conseil de sécurité intérieure »*[59]. Ce conseil dont il est question tiendrait des réunions annuelles qui auraient lieu quatre fois par an entre les chefs d'Etats et de gouvernement pour assurer une meilleure coordination à l'échelle européenne, tel que l'Eurogroupe sur les questions financières pour la zone euro[60]. Ce conseil aurait trois objectifs : l'évaluation du contrôle des frontières, l'échange d'informations qui permettrait une meilleure coordination ainsi que la sanction des Etats qui ne respecteraient pas leurs obligations en cas de manquements répétées. Cependant il est nécessaire de s'interroger sur l'effectivité de cette proposition. En effet, l'Eurogroupe subit actuellement les résistances des Etats membres. Ainsi, le risque majeur de ce Conseil de sécurité intérieur est la paralysie en raison des intérêts divergents entre Etats. Cette instance ne pourrait alors avoir qu'un rôle de concertation, de négociation. En outre, le fait de pouvoir sanctionner ses pairs apparaît être difficile à mettre en œuvre en raison de certaines alliances politiques. De plus, les Etats membres consentiraient-il à une majorité qualifiée ? La sanction au profit de l'entraide ne risque-t-elle pas d'aggraver les problématiques de méfiance des Etats à l'égard des autres ? Ces propositions et soutiens qui ont suivi, notamment de la part de l'Allemagne, ont eu le mérite de susciter un réel débat sur l'avenir de l'espace Schengen et pousser les institutions de l'Union européenne

[58]https://www.elysee.fr/emmanuel-macron/2020/11/05/je-suis-favorable-a-une-refondation-complete-de-schengen-deplacement-du-president-emmanuel-macron-dans-les-pyrenees-orientales
[59] https://www.elysee.fr/emmanuel-macron/2020/11/10/conference-de-presse-conjointe-sur-la-reponse-europeenne-a-la-menace-terroriste
[60] https://www.lopinion.fr/edition/international/espace-schengen-propositions-d-emmanuel-macron-reforme-230600

à s'emparer du sujet. En effet, ces dernières ont décidé d'organiser un forum Schengen qui a abouti à la « Stratégie Schengen » ayant pour objectif de rendre l'espace plus résilient.

2. Rendre l'espace Schengen résilient : Stratégie Schengen 2021

21.- Forum Schengen – Ursula Von der Leyen, Présidente de la Commission européenne, a fait une constatation claire sur l'état actuel de l'espace Schengen : *« les premiers mois de la pandémie nous ont montré ce qui se produit lorsque Schengen s'arrête de fonctionner : l'Europe se paralyse »*[61]. Devant l'accord des dirigeants des Etats membres sur le besoin de renforcement de l'espace Schengen, le 30 novembre 2020 a eu lieu le premier forum Schengen. Tous les ministres de l'Intérieur de l'Union et la Commissaire aux affaires intérieures, Ylva Johansson, ont été convoqués par la Commission européenne avec un objectif commun : rendre l'espace Schengen *« plus renforcé et plus résilient »*. Durant ce forum, les priorités ont été abordées tels que le besoin d'encadrer davantage le rétablissement temporaire des contrôles aux frontières intérieures tout en prenant en compte les menaces actuelles, l'urgence d'intensifier les contrôles grâce à l'interopérabilité des bases de données, la coopération et l'échange d'information et améliorer le mécanisme d'évaluation des principes de Schengen. A l'issue de ce forum, Ursula Von der Leyen a annoncé que la Commission européenne présentera mi-2021 une stratégie pour renforcer l'espace : la Stratégie Schengen.

22.- Stratégie Schengen – Comme annoncé, le 02 juin 2021, la Commission européenne présente sa stratégie pour tenter de surmonter les difficultés existentielles que connaît l'espace Schengen tout en rappelant l'importance de cette architecture *: « La liberté de se déplacer, de vivre et de travailler dans différents Etats membres est une liberté chère au cœur des Européens. Elle est l'une des plus grandes réussites de l'Union mais diverses crises et problèmes nous ont montré que nous ne pouvons pas considérer l'espace Schengen comme acquis. Aujourd'hui, nous présentons une voie qui permettra à l'espace Schengen de résister à l'épreuve du temps, qui garantira la libre circulation des personnes, des marchandises et des services en toutes circonstances, pour reconstruire nos économies et pour qu'ensemble, nous sortions plus forts de cette épreuve »*[62]. C'est donc bien un message conquérant et d'optimisme qui est adressé aux Etats membres attirés par l'isolement et la résignation. L'un des premiers souhaits des Etats membres a été entendu puisque cette importante réforme prévoit une révision du mécanisme d'évaluation de Schengen plus offensif. La Commission prévient que des poursuites

[61] https://www.etiasvisa.com/fr/actualites/ue-revision-espace-schengen
[62] Communication 02/06/2021 from the Commission to the European Parliament and the Council "A strategy towards a fully functioning and resilient Schengen area"

judiciaires auront lieu en cas de manquements répétées aux règles et des visites inopinées dans les Etats pourront avoir lieu contrairement à la nécessaire annonce en amont de 24 heures. Le manque d'effectif constaté notamment aux frontières et aux côtes sera comblé par l'arrivée de 10 000 agents supplémentaires. En outre, la Commission mise sur l'interopérabilité des bases de données et une coopération plus étroite entre les Etats grâce à la création d'un code de coopération policière européen et la tenue régulière de forums Schengen qui auront pour but de favoriser le dialogue. Une révision du Code frontière Schengen est également annoncée.

23.- L'élargissement de l'espace Schengen – Dans la présentation de la réforme, Ursula Von der Leyen a également exprimé sa volonté d'élargir l'espace Schengen à la Bulgarie et la Roumanie considérant qu'une gestion plus efficace des frontières extérieures ne pourra se faire sans eux. Au regard du développement d'une méfiance mutuelle, les Etats sont-ils prêts à accepter pleinement ces nouveaux partenaires ? La corruption, la précarité économique de ces pays, leur capacité à surveiller les frontières cristallisent toutes les préoccupations, comme mis en avant par le Premier Ministre hollandais, Mark Rutte[63]. Il leur est notamment reproché leur proximité avec la Grèce et la Turquie, il est urgent de les associer afin de mieux maîtriser les flux et d'obtenir toutes les informations nécessaires. L'unanimité sera nécessaire pour inclure entièrement ces pays dans l'espace.

[63] G. Georgi « Rutte pours cold water on Bulgaria's Schengen and Eurozone dreams", *Euractiv*, 07/02/2018

Chapitre II. Les mutations engendrées par un système électronique d'autorisation de voyage

La mise en place du système électronique d'autorisation de voyage (I) engendre un impact important auprès des principaux acteurs (II).

Section I. La mise en place de l'ETIAS

La mise en place de l'ETIAS nécessite d'étudier son champ d'application (I), sa structure (II) et la procédure de délivrance d'une autorisation de voyage (III).

I. Un objectif justifiant le champ d'application

24.- Objectifs – Lors du discours sur l'état de l'Union, le 14 septembre 2016, Jean-Claude Juncker, Président de la Commission européenne entre 2014 et 2019, a clairement énoncé l'objectif de la mise en place de cette autorisation de voyage et plus généralement des bases de données : *« Nous devons savoir qui traverse nos frontières. De cette façon, nous saurons quelles sont les personnes qui voyagent vers l'Europe avant même qu'elles n'arrivent ici »*[64]. Et pour cause, 20% des ressortissants des pays tiers qui arrivent sur le sol européen ne sont pas contrôlés en amont, ce qui signifie qu'aucune étude ne peut être réalisée quant à l'éventuel risque que constituent ces individus. Le manque d'information et l'absence d'analyse de risque poussent donc aujourd'hui les dirigeants à la mise en place de l'ETIAS. Cette base de données est instaurée par le Règlement 2018/1240[65] ainsi que trois décisions déléguées[66]. Son article 4 est relatif aux objectifs de l'ETIAS qu'il peut être possible de résumer en trois axes : la prévention des infractions, de l'immigration illégale et de la santé publique, assurer un *« niveau élevé de sécurité »* qui permet un contrôle des frontières plus efficace et le renforcement des objectifs du SIS. Certains s'interrogeront sur le fait de créer une base de données supplémentaire, ce qui implique des procédures et règles supplémentaires alors qu'existe le visa Schengen. Pourquoi ces ressortissants ne seraient-ils pas soumis aux obligations d'un visa de courte durée ? Il est nécessaire de rappeler que le visa uniforme a pour objectif de faire une étude approfondie du demandeur, avec des pièces justificatives supplémentaires, ce qui implique un temps de procédure plus long. Or, les ressortissants de ces pays ont un risque migratoire faible par rapport à ceux soumis à cette formalité. Il apparaît donc inutile d'alourdir les procédures et rallonger ce temps d'analyse. Quant à la question de la

[64] https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_16_3043
[65] Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[66] Décision n°2019/969 et Décision n°2019/970 de la Commission européenne du 22 février 2019 et la Décision n°2020/971 de la Commission du 26 février 2019

protection de la santé publique, elle peut être étudiée également avec l'ETIAS car aujourd'hui le raisonnement ne se fait pas individuellement mais par pays, voire par région du monde. Il sera donc possible d'interdire l'accès à l'espace Schengen à une population en raison d'un virus qui sévirait dans ce pays. Ainsi, tous ces objectifs expliquent le champ d'application de ce Règlement.

25.- Champ d'application – L'article 2 du Règlement 2018/1240 évoque son champ d'application. Ainsi, l'ETIAS est applicable aux ressortissants de pays tiers qui ne sont pas soumis à l'obligation d'obtention d'un visa, en vertu de l'annexe II du Règlement 539/2001[67], aux écoliers ressortissants d'un pays tiers soumis à l'obligation de visa qui effectuent un voyage scolaire organisé et aux membres de la famille d'un citoyen de l'Union européenne qui ne disposent pas de carte de séjour[68] ou de titre de séjour[69]. L'ETIAS concerne principalement les pays du continent américain, l'Australie et quelques pays asiatiques. Il devrait entrer en vigueur mi-2022. Une période transitoire de six mois sera instaurée c'est-à-dire jusqu'à début 2023. Ainsi, les voyageurs pourront faire la demande d'autorisation de voyage sans que cela ne soit obligatoire.

II. La structure à deux niveaux de l'ETIAS

L'ETIAS est composé d'une unité centrale créée au sein de l'Agence européenne de garde-frontières et de garde-côtes (A) ainsi que d'une unité nationale dans chaque Etat membre (B).

A. L'unité centrale ETIAS : FRONTEX

L'Agence européenne de garde-frontières et de garde-côtes, dite FRONTEX, dispose de nouvelles prérogatives lui permettant d'accroitre son poids sur la scène européenne (2) alors qu'originellement plusieurs facteurs limitaient sa pleine expansion (1).

1. Les limites initiales d'une agence européenne au centre de la surveillance des frontières extérieure

26.- Avant 2016 - En 2002, la Commission européenne propose la création de garde-frontières européens. Mais ce projet est refusé par les Etats qui craignent pour leur

[67] Règlement (CE) n°539/2001 du Conseil du 15 mars 2001 fixant la liste des pays tiers dont les ressortissants sont soumis à l'obligation de visa pour franchir les frontières extérieures des Etats membres et la liste de ceux dont les ressortissants sont exemptés de cette obligation
[68] Directive 2004/38/CE 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 Etats membres
[69] Règlement (CE) n° 1030/2002 du Conseil du 13 juin 2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers

souveraineté. Un travail de longue haleine va s'amorcer, aboutissant par la création de l'Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des Etats membres instituée par le Règlement 2007/2004[70], le 26 octobre 2004. Son objectif est de soutenir les Etats membres dans leur prérogative de protection des frontières extérieures tout en renforçant la coordination et la coopération opérationnelle entre eux. Les Etats ont cependant été très réticents à cette agence, au départ, puisqu'ils ont souhaité faire inscrire dès l'article 1 paragraphe 2 dudit Règlement que l'agence n'est pas responsable de la protection des frontières de l'Union qui reste une mission assurée par les Etats membres. Outre cette défiance, les capacités financières et techniques limitées, vont considérablement borner les actions de l'agence qui ne se contentera durant cette période que d'un rôle de coordination et de concertation[71]. En effet, l'agence va uniquement avoir comme mission de tenir un registre énumérant les équipements de contrôle et du surveillance disponibles pour les Etats. Les différentes crises migratoires de la première décennie vont accroitre les besoins des Etats membres et démontrer son inefficacité, ce qui va permettre à l'agence dès 2016, de prendre une place un peu plus importante dans le contrôle des frontières.

27.- Depuis 2016 – Ainsi, le Règlement 2016/1624[72], du 14 septembre 2016, créé l'Agence européenne de garde-frontière et de garde-côtes, dénommée FRONTEX[73]. Cette réforme bouleverse les prérogatives de l'agence puisqu'à partir de 2016, un régime de responsabilité et de solidarité est instauré, une augmentation significative de son budget et de son effectif est décidée et surtout FRONTEX peut désormais disposer de prérogatives à la place d'un Etat membre défaillant. L'agence ne dépend plus du bon vouloir des Etats, elle devient autonome sans toutefois empiéter sur la souveraineté des Etats, sauf si ces derniers ne remplissent pas leurs obligations. En effet, chaque Etat membre est tenu de mettre à disposition un vivier de 2% de ses effectifs de garde-frontières et garde-côtes et de 3% si l'Etat ne dispose pas de frontière extérieure[74]. Contrairement à 2004, la protection des frontières extérieures est assurée par les Etats mais aussi l'agence. L'opération Triton[75], menée en Italie et l'opération Poséidon[76], en

[70] Règlement (CE) n° 2007/2004 du Conseil du 26 octobre 2004 portant création d'une Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des Etats membres de l'Union européenne
[71] A. KARGL, « FRONTEX, symbole d'une gestion des frontières européennes en évolution », publié par l'ANAJ-IHEDN, 1 mars 2018
[72] Règlement (UE) n° 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes
[73] https://frontex.europa.eu/fr/
[74] Rapport d'information de l'Assemblée Nationale des Députés Ludovic MENDES et Christophe NAEGELEN, L'espace Schengen et la maîtrise des frontières extérieure de l'Union européenne, 19 avril 2018
[75] Opération menée par FRONTEX, ayant eu lieu entre novembre 2014 et janvier 2018 et qui avait pour but de surveiller les frontières au large de Lampedusa grâce à la mutualisation de matériel technique et de gardes-frontières
[76] Opération menée par FRONTEX, ayant eu lieu en 2015, a permis de fournir une assistance technique pour la surveillance entre les frontières grecques et turques et le sauvetage en mer de migrants

Grèce sont des exemples de cette collaboration[77]. FRONTEX a également obtenu la possibilité de travailler avec les pays tiers et notamment de coordonner les réadmissions des individus qui tentent d'entrer dans l'espace Schengen sans être conforme aux réglementations en vigueur. La volonté de pousser les Etats à travailler avec l'agence a aussi été mise en place, le 02 décembre 2013, par EUROSUR[78]. Il est un instrument d'échanges d'informations opérationnelles, en temps réel, permettant ainsi de mieux cibler les actions sur les frontières extérieures. FRONTEX est une agence en pleine mutation dont le mandat est une nouvelle fois renforcé grâce à la mise en place de l'ETIAS, ce qui lui permet de renforcer son rôle.

2. Des nouvelles prérogatives pour renforcer le poids de cette agence

28.- Trois nouvelles missions- L'article 7 du Règlement instituant l'ETIAS est relatif à l'unité centrale qui sera créée au sein de FRONTEX. Les nouvelles missions confiées à cette agence sont de trois ordres. FRONTEX doit veiller au respect des droits fondamentaux et en particulier du respect au droit à la protection des données personnelles et au respect de la vie privée. Pour cela, des audits réguliers devront être menés par cette agence afin d'évaluer les conséquences de la mise en place de l'ETIAS sur ces droits. Elle vérifie également si les données à caractère personnel du demandeur correspondent à la personne à qui l'acceptation a été délivrée, et ce en analysant les bases de données et les données d'Europol et Interpol. FRONTEX a un rôle d'informateur, en collaboration avec la Commission européenne, auprès des transporteurs aériens et des unités nationales en cas de dysfonctionnement, mais également auprès du public. Enfin, un rapport d'activité annuel devra être rédigé pour les institutions européennes.

B. L'unité nationale ETIAS

29.- Désignation d'une autorité nationale compétence – L'article 8 paragraphe 1 du Règlement 2018/1240 dispose que *« chaque Etat membre désigne une autorité compétente comme unité nationale ETIAS »*. Celle-ci aura pour mission d'examiner les demandes d'autorisation de voyage qui ont obtenu une réponse positive, les demandes d'autorisation de voyage à validité territoriale limitée et annuler et révoquer des autorisations de voyage.

[77] https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/securing-eu-borders/fact-sheets/docs//eu_operations_in_the_mediterranean_sea_fr.pdf
[78] https://www.touteleurope.eu/societe/qu-est-ce-qu-eurosur/

III. La procédure de délivrance d'une autorisation de voyage

A. L'examen de la demande

30.- Introduction de la demande en ligne – Comme mentionné par les articles 15 et 16 du Règlement 2018/1240, la demande d'une autorisation de voyage ne peut s'effectuer qu'en ligne, soit par le site internet soit par une application pour appareil mobile. Cette demande dématérialisée est gratuite mais nécessite donc de posséder une connexion internet et de savoir utiliser les outils informatiques. Les individus possédant déjà une autorisation de voyage ne peuvent renouveler leur demande qu'à compter de 120 jours avant son expiration. Cette demande est personnelle car elle ne peut être effectuée que par la personne concernée ou par un *« intermédiaire commercial autorisé par le demandeur »*[79] ce qui renvoi en particulier aux agences de voyages pour l'organisation d'un séjour en Europe. Pour effectuer une demande d'ETIAS, chaque demandeur doit compléter trois documents[80] : le formulaire de demande, une déclaration d'authenticité, d'exhaustivité, d'exactitude et de fiabilité des données fournies ainsi qu'une déclaration de véracité et de fiabilité de ses déclarations. Un nombre important de données à caractère personnel sont à indiquer sur l'identité du demandeur, sa formation scolaire et vie professionnelle et sur ses intentions de résidence en Europe. Trois questions lui sont en outre posées, à savoir *« s'il a été condamné pour une infraction, s'il a séjourné dans une zone de guerre ou de conflit particulière et s'il a fait l'objet d'un ordre de quitter le territoire d'un Etat membre ou de tout pays tiers »*[81]. Ces interrogations sont révélatrices de la volonté des autorités d'évaluer l'éventuel risque de l'individu d'un point de vue de la sécurité publique ou s'il pourrait venir en Europe pour y effectuer une demande d'asile. Chaque requérant devra verser la somme de 7 euros à l'exception de ceux âgés de moins de 18 ans ou de plus de 70 ans[82]. Un mail est adressé sur l'adresse email renseignée à la fin de la création de la demande.

31.- Traitement automatisé de la demande – Toutes les données fournies par le demandeur sont automatiquement comparées à toutes les bases de données de l'Union, à savoir le SIS, le système entrée/sortie (EES), le système d'information sur les visas (VIS), Eurodac, la liste de surveillance ETIAS, les données d'Europol et les bases de données

[79] Article 15 paragraphe 4 Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[80] Article 17 paragraphe 1 Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[81] Article 17 paragraphe 3 Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[82] Article 18 Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

d'Interpol à savoir SLTD et TDAWN[83] *(cf. paragraphes 52 à 55).* Le système central ETIAS est à l'affût de toute réponse positive pour savoir si par exemple le document de voyage renseigné est signalé comme volé, détourné ou invalidé, si l'identité du demandeur correspond à un mandat d'arrêt européen ou à un signalement de non-admission et d'interdiction de séjour ou encore si l'identité du demandeur correspond à une personne qui est connue des autorités pour avoir déjà dépassé la durée du séjour autorisée dans l'espace Schengen. La majorité des dossiers s'arrêteront à ce stade car n'ayant aucune correspondance avec les renseignements détenus par l'Union. Une autorisation de voyage sera alors délivrée automatiquement. Dans le cas contraire, si une ou plusieurs correspondances ressortent ou si le demandeur a répondu par l'affirmative à l'une des trois questions ou si des doutes subsistent alors une vérification par l'unité centrale est effectuée.

32.- Vérification de la demande par l'unité centrale – L'unité centrale, située au sein de FRONTEX, effectue une seconde recherche pour savoir si la correspondance est bien existante et de quel type est-elle. En cas d'erreur, l'autorisation de voyage sera automatiquement délivrée après avoir supprimée la correspondance erronée. Si une ou plusieurs réponses positives persistent ou si des doutes perdurent alors un traitement manuel sera effectué par l'unité nationale[84].

33.- La détermination de l'Etat membre responsable du traitement – Pour savoir quelle unité nationale aura la charge d'étudier manuellement le dossier, l'Etat membre responsable doit être déterminé[85]. Cet Etat responsable est l'Etat qui a introduit ou fourni les renseignements qui ont déclenché la correspondance dans les autres bases de données. Si plusieurs Etats ont effectué un signalement sur l'individu alors l'Etat responsable est celui qui a fourni les données les plus récentes. En cas de traitement manuel qui résulte de doutes et non d'une correspondance, l'Etat membre responsable est l'Etat membre d'entrée dans l'espace Schengen. L'unité centrale transmet à l'unité nationale déterminée la raison qui nécessite un traitement manuel. Si l'une des correspondances met en avant que le document de voyage est volé, détourné ou invalidé ou que l'individu fait l'objet d'un signalement de non-admission et interdiction de séjour dans l'espace Schengen alors l'unité nationale devra nécessairement refuser l'autorisation de voyage. Si elle est relative à un autre domaine alors l'unité nationale procède à une évaluation du risque en matière de sécurité et d'immigration illégale. Pour ce faire, l'unité nationale peut exiger des

[83] Article 20 Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[84] Article 26 du Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[85] Article 25 du Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

informations ou documents nécessaires pour son analyse. Le demandeur dispose de dix jours pour délivrer ces pièces. Le Règlement précise que *« dans des circonstances exceptionnelles »*[86], l'unité nationale pourra faire passer un entretien dans le consulat du pays de résidence du demandeur ou en visioconférence si les documents transmis sont insuffisants à l'analyse du risque. Si l'individu ne se présente pas à cet entretien alors l'unité nationale refusera l'autorisation de voyage. L'unité nationale peut à tout moment délivrer l'autorisation de voyage si elle estime que le risque est mineur.

34.- Consultations des autres Etats membres et Europol – Pour l'aider dans son analyse du risque, l'unité nationale peut consulter les autres Etats membres qui auraient aussi effectué un signalement dans l'une des bases de données. Un avis doit être nécessairement rendu par ces Etats. Dans le cas d'un avis négatif d'au moins un des Etats, l'unité nationale devra refuser l'autorisation de voyage. Cela n'est pas le cas quant à la consultation d'Europol qui n'a qu'un avis consultatif.

35.- Délais – A partir de l'introduction d'une demande d'autorisation de voyage, les autorités disposent de 96 heures pour autoriser, refuser ou demander des documents supplémentaires au demandeur. Dans ce dernier cas, un nouveau délai de 96 heures s'ouvre à compter de la transmission des pièces demandées[87].

36.- Particularités pour les membres de la famille d'un citoyen de l'Union – Quand le demandeur est un membre de la famille d'un citoyen de l'Union ou un ressortissant de pays tiers qui dispose d'une libre circulation, le Règlement prévoit[88] qu'il ne sera pas vérifié si l'individu a déjà dépassé la durée du séjour autorisé, ni si ses données correspondent à la base de données Eurodac. Il est également indiqué que ces individus ne peuvent se voir refuser une autorisation de voyage au motif d'un risque d'immigration illégale. Cette dernière précision peut être critiquable car la qualité de membre de la famille d'un citoyen de l'Union n'exclut pas la possibilité d'une immigration illégale. Certes, cette catégorie d'individus bénéficie par la Directive de 2004 de droits et facilités pour entrer sur le territoire Schengen, mais aucune disposition à ce jour ne leur permet de rester dans l'un des Etats membres en dépassant les délais autorisés.

[86] Article 27 paragraphe 4 du Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[87] Article 30 et 32 du Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[88] Article 24 du Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

B. Le réexamen possible d'une autorisation de voyage délivrée

37.- Délivrance - L'autorisation de voyage peut être délivrée avec une mention demandant aux autorités frontalières de procéder à une vérification quand l'individu se présentera devant eux. Cette mention est supprimée du dossier dès que le second contrôle est effectué. L'ETIAS est valable pendant trois ans ou jusqu'à la fin de la validité du document de voyage qui a été indiqué.

38.- Annulation et révocation – Le réexamen du dossier du demandeur est toujours possible même après la délivrance de l'ETIAS. En effet, si au cours de la période de validité de l'ETIAS, l'un des Etats membre s'aperçoit que les conditions de délivrance de l'autorisation de voyage n'étaient pas remplies au moment de la demande et qu'il peut le prouver, alors l'unité nationale de cet Etat pourra annuler l'autorisation de voyage. En outre, si une nouvelle correspondance émerge durant la période de validité de l'autorisation de voyage alors le système central ETIAS informe l'unité nationale de ce nouvel élément. Une nouvelle étude du dossier a lieu. Cependant, il faut s'interroger sur la révocation ou l'annulation de l'autorisation de voyage lorsque l'étranger est déjà sur le territoire de l'un des Etats membre de l'espace, quelle est la marge de manœuvre des autorités ? La révocation peut également avoir lieu conformément à la volonté de l'intéressé. Le demandeur dispose d'un droit de recours en cas d'annulation ou de révocation de son ETIAS, sauf si celle-ci a lieu à son initiative[89].

Section II. L'impact de l'instauration de l'ETIAS pour le transporteur aérien sur le régime français des passagers non-admissibles

L'abandon par l'Etat de ses prérogatives de puissance publique crée une lourde responsabilité portée par le transporteur aérien (I), notamment causée par la problématique épineuse de la vérification documentaire manuelle (II).

I. L'abandon par l'Etat de ses prérogatives de puissance publique au profit d'une lourde responsabilité du transporteur aérien

39.- Obligation de vérification documentaire – L'article L 6421-2 du Code des transports fait peser sur le transporteur une obligation de contrôle documentaire, c'est-à-dire qu'il doit préalablement, à l'embarquement, vérifier que ses passagers détiennent bien les documents nécessaires pour entrer en France. En cas de manquement, une

[89] Chapitre VI du Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

sanction financière, existe et ne cesse d'être augmentée. En effet, alors que le montant de l'amende était fixé à 1 500 euros[90], elle est augmentée à 5 000 euros en 2003[91] puis à 10 000 euros en 2016[92]. Avant cette date, il existait une réduction de l'amende si le transporteur aérien avait mis en place un dispositif de numérisation et de transmission des documents de voyage mais l'article L 625-3 du Code de l'entrée et du séjour des étrangers et du droit d'asile (ci-après « CESEDA ») a été abrogé par la loi de 2016[93]. Dans la pratique, seuls les passagers provenant d'un pays hors Schengen sont concernés par cette potentielle amende. L'annexe 9 de l'OACI[94] prévoit que les Etats doivent aider les transporteurs aériens dans la vérification documentaire et n'impute aucune responsabilité à l'égard de ces derniers puisque cette obligation pèse sur les gardes-frontières d'après l'article 8 du Code frontières Schengen.

40.- Obligation d'information et de conseil - La jurisprudence considère que le transporteur aérien n'a pas d'obligation d'information et de conseil quant aux formalités d'entrée et de séjour dans l'Etat de destination[95], contrairement aux agences de voyage[96]. Cependant, pour des raisons commerciales et pour éviter des refus d'embarquement, certaines compagnies aériennes. Cette volonté d'information s'est notamment accentuée avec la pandémie de la Covid-19. En effet, certains pays exigent désormais des voyageurs qu'ils remplissent des formulaires de localisation ou qu'ils effectuent des tests antigéniques ou PCR avant le départ. Le manque d'harmonisation entre les différents pays européens complexifie cette vérification.

41.- Obligation de réacheminement - Le transporteur est également soumis à une obligation de réacheminement sanctionnée par une amende pouvant aller jusqu'à 30 000 euros en cas de manquement[97]. Le tribunal administratif considère que le transporteur aérien doit *« mettre en œuvre des procédures internes en vue d'assurer la sécurité des avions et de leurs occupants dans les cas de transports de passagers non admissibles ou refoulés »*[98]. En effet, le défaut de réacheminement est le plus souvent causé par la résistance, parfois violente, de l'individu qui ne souhaite pas être ramené dans son pays d'origine. Le transporteur doit à la fois réacheminer le passager non-admissible (ci-après « INAD ») tout en préservant la sécurité du vol, et pour ce faire prévoir l'éventuel refus

[90] Article 20 bis de la loi n°92-190 du 26 février 1992 relative aux conditions d'entrée et de séjour des étrangers en France
[91] Article 27 de la loi n°2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité
[92] Loi n°2016-274 du 07 mars 2016 relative au droit des étrangers en France
[93] Cours de Droit aérien, Madame LABORDE DIT BOURIAT, année universitaire 2020-2021
[94] Annexe 9 de la Convention relative à l'aviation civile internationale, « Facilitation », Octobre 2017
[95] Cass, civ. 1e , 10 septembre 2015 n°14-22.223
[96] Cass, civ. 1e ,19 mars 2009, n°08-11617
[97] Article L 625-7 du Code de l'entrée et du séjour des étrangers et du droit d'asile
[98] Tribunal administratif de Paris, 26 février 2019, n°1711819/3-1

de l'individu. En outre, il est nécessaire de rappeler que le commandant de bord peut débarquer toute personne qui constituerait un risque pour la sécurité[99]. Ainsi, le commandant de bord a légalement la possibiliser de refuser le transport d'un INAD[100] qui constituerait une menace à cet égard. Un débat entre l'Etat et les transporteurs existe en ce qui concerne l'escorte. Doit-elle être mise en place par la compagnie ou bien par l'Etat qui est le seul à pouvoir faire usage de la force ?[101].

42.- Obligation de prise en charge – Etant responsable de la venue du passager non-admis, le transporteur doit également assurer sa prise en charge à compter de la prononciation du refus d'entrer, tel qu'envisagé par l'article L 213-6 du CESEDA. Cela renvoie à l'hébergement, l'alimentation ou d'éventuels frais médicaux. L'exonération de la responsabilité du transporteur ne peut avoir lieu que si l'étranger a obtenu une demande d'asile et cesse durant l'examen de la demande.

43.- Poids financier des INAD pour Transavia France – A titre d'exemple, la compagnie aérienne Transavia France a dû faire face à un risque financier de près d'un million d'euros en 2019 sur environ 100 dossiers[102]. Légalement, il existe des moyens pour faire diminuer cette charge financière. En effet, les Conditions Générales de Vente et de Transport (ci-après « CGV ») peuvent exiger du passager non-admissible le remboursement des frais engagés, tel est le cas de ceux de la compagnie aérienne Lufthansa[103]. Cependant, cela s'avère matériellement impossible. En effet, dans la majorité des cas, ces passagers ne sont pas solvables donc il est impossible d'obtenir le recouvrement de cette créance. En outre, pour des raisons commerciales cette exigence peut être discutable. C'est la raison pour laquelle une telle disposition n'existe pas dans les CGV du transporteur Transavia France. La dernière option possible pour les compagnies est d'user des levées contractuelles avec leurs handlers[104] afin de partager ces frais.

[99] Article 6.1 de la Convention relative aux infractions et à certains autres actes survenant à bord des aéronefs, 14 septembre 1963 et Article L 6522 – 3 du Code des transports

[100] Règlement (CE) n°859/2008 de la Commission du 20 août 2008 en ce qui concerne les règles techniques et procédures administratives communes applicables au transport commercial par avion

[101] Mémoire de Julie DURAFFOURD, « Le transport par air de passagers non admissibles », années universitaire 2018-2019

[102] Documents de travail du service juridique de Transavia France

[103] https://www.lufthansa.com/fr/fr/conditions-generales-1

[104] D'après le Dico du commerce international « En logistique aérienne, l'agent de handling est une entreprise assurant, moyennant rémunération, certaines opérations matérielles, commerciales ou douanières, pour le compte d'un transporteur ne possédant pas d'installations dans l'aéroport où elle exerce son activité »

II. La problématique épineuse de la vérification documentaire manuelle

La mise en place d'un portail des transporteurs (A) démontre qu'une solution est possible pour rendre le contrôle documentaire efficace et ainsi faire baisser le nombre de passagers non-admissibles sur le territoire français (B).

A. L'accès au système d'information ETIAS par le portail des transporteurs

44.- Fonctionnement du portail - L'article 45 paragraphe 1 du Règlement qui institue l'ETIAS[105] dispose que *« les transporteurs aériens (…) interrogent le système d'information ETIAS afin de vérifier si les ressortissants de pays tiers soumis à l'obligation d'être munis d'une autorisation de voyage sont ou non en possession d'une autorisation de voyage en cours de validité »*. Ainsi, à l'exception du cas de transit aéroportuaire, les transporteurs aériens sont tenus de vérifier si leurs passagers disposent d'un ETIAS pour pouvoir accéder à l'espace Schengen. Ainsi, le transporteur aérien n'a pas un accès au dossier ETIAS lui-même mais à une *« base de données distincte en lecture seule mise à jour quotidiennement au moyen d'une extraction à sens unique »*, qui permet par un système simple de « ok » ou « not ok » de savoir si l'autorisation de voyage a bien été délivrée et si celle-ci est toujours valide. Le transporteur est en mesure de conserver la réponse reçue, ce qui pourrait être utile en cas de contentieux. En cas d'autorisation de voyage à validité territorialement limitée, la réponse prend en compte également si l'individu peut se rendre dans le pays de destination. En outre, le Règlement mentionne qu'un « dispositif d'authentification » sera mis en place afin de circonscrire le nombre de personnes habilitées à obtenir cette information. En cas de dysfonctionnement du portail, *« les transporteurs sont exemptés de l'obligation de vérifier les voyageurs en possession d'une autorisation de voyage en cours de validité »*[106]. Cela signifie-t-il que l'Etat assumera la responsabilité d'un éventuel INAD en cas de défaillance du portail dont l'agence européenne eu-LISA assure la gestion opérationnelle ? Ces cas resteront malgré tout limités.

45.- Des sanctions toujours applicables – Bien que le contrôle documentaire se fasse par l'Etat qui donne dans un second temps l'instruction au transporteur aérien de laisser ou non embarquer le passager soumis à l'obligation de détention d'un ETIAS, l'article 45

[105] Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[106] Article 46 du Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

paragraphe 5 du Règlement[107] dispose que les transporteurs aériens peuvent être sanctionnés, s'ils transportent des voyageurs qui ne détiennent pas d'autorisations de voyage conformes pour entrer sur le territoire de l'espace Schengen. En outre, le paragraphe 8 dudit article prévoit que l'obligation de prise en charge et le défaut de réacheminement sont sanctionnés. Les sanctions à l'égard du transporteur aérien sont toujours d'actualité dans les textes. Or, le transporteur suivra nécessairement l'information obtenue depuis ce portail. En conséquence, la possibilité qu'un ressortissant d'un pays tiers soumis à l'obligation de détention d'un ETIAS devienne un INAD devient faible. Ainsi, la responsabilité et le coût financier qu'ils représentent pourront sensiblement décroitre pour cette catégorie de passagers.

B. Une possible solution pour une vérification documentaire efficace

46.- Exonération de la responsabilité du transporteur – Le principal moyen de défense du transporteur aérien sur son obligation de vérification documentaire est l'absence d'irrégularité manifeste à l'embarquement, prévu par l'article L 625-5 du CESEDA. Le transporteur doit apporter la preuve que l'irrégularité ne pouvait être relevée de manière évidente, sans contrôle plus approfondit ou par l'utilisation de techniques supplémentaires. Cela peut être le cas en cas de documents de voyage falsifiés ou d'usurpation d'identité. L'irrégularité manifeste n'étant pas clairement définie ni par les textes, ni par la jurisprudence, une marge d'appréciation créée un débat sur cette notion[108].

47.- Vers une vérification numérique – La mise en place de l'ETIAS est un réel tournant dans le contrôle documentaire de voyage. En effet, il est nécessaire de rappeler que les visas Schengen sont aujourd'hui contrôlés de manière manuelle. Cette vérification, qui doit être de surcroit rapide, fait l'objet d'une complexité importante induisant nécessairement des erreurs. La police aux frontières ainsi que les agents d'une compagnie doivent vérifier les cachets d'entrée et de sortie qui ne sont pas toujours visibles ou dans le même sens, calculer mentalement si la durée de séjour n'excède pas les 90 jours sur une période de 180 jours. La vérification numérique des visas Schengen, à l'instar de l'ETIAS, permettrait de réduire considérablement le nombre d'INAD et par conséquent la responsabilité du transporteur aérien et le poids financier que cela représente.

[107] Article 45 paragraphe 5 du Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[108] Mémoire de Julie DURAFFOURD, « Le transport par air de passagers non admissibles », année universitaire 2018-2019

Titre II - Des systèmes d'information collectant un nombre grandissant de données à caractère personnel

L'établissement des systèmes d'information européens et le développement de l'interopérabilité s'impose aujourd'hui comme la solution aux lacunes de l'espace Schengen (I). Cette montée en puissance du nombre de données à caractère personnel permet à l'agence européenne Eu-LISA d'être au cœur de cette gestion (II).

Chapitre I. La solution de l'interopérabilité des systèmes d'information

L'ETIAS compare les données à caractère personnel du demandeur avec les données comprises dans divers systèmes d'information européens en pleine expansion (I). La mise en place de l'interopérabilité est un effet multiplicateur du traitement de données à caractère personnels (II)

Section I. Une collecte de données existantes par des systèmes d'information en pleine expansion

Différents systèmes d'information européens ont été mis en place (I) par les institutions avec un objectif commun qui s'avère être de plus en plus gourmand, ce qui explique leurs expansions (II).

I. La notion de système d'information

48.- Définition – Avant de développer sur les différents systèmes d'information européens existants, il est nécessaire de ne pas confondre la notion de bases de données et celle de systèmes d'information qui pourraient cependant apparaître comme synonymes. En effet, *« une base de données n'est qu'un conteneur stockant des éléments discrets (chiffres, dates, images) pouvant être retraités par des moyens informatiques afin de produire une sortie significative. Un système d'information est un objet bien plus complexe qui organise des ressources ou entrées (personnel, procédures, matériels, logiciels) permettant d'acquérir, de stocker, de structurer et d'échanger – transmettre ou recevoir – parmi des sujets autorisés des informations pertinentes provenant de différentes sources et destinées à servir de base aux décisions »*[109].

[109] G.Serra et R. Angrisani, « Espace Schengen et Systèmes d'information : le rôle de l'agence Eu-LISA », Février 2016

49.- Composition identique des systèmes d'information – Chaque système d'information, à l'instar d'ETIAS, possède la même architecture. En effet, ces systèmes sont tous constitués d'une unité centrale principale, d'une unité centrale de secours permettant de prendre la relève de l'unité centrale en cas de défaillance de celui-ci, de fichiers nationaux dont chaque Etat membre est responsable et enfin d'une unité de communication qui permet la transmission sécurisée des données recherchées.

50.- Distinction temporelle – Les systèmes d'information européens peuvent être distingués par leur temporalité. En effet, Eurodac, le système d'information sur les visas (SIS) et les bases de données Interpol dont le SLTD et TDAWN sont les toutes premières développées par l'Union européenne. Avides de plus d'informations et motivés par de nouvelles menaces, les Etats ont souhaité établir et développer de nouveaux systèmes d'information tels que le système européen d'information sur les casiers judiciaires (ECRIS) et tout récemment le système entrée/sortie (EES), l'ETIAS et sa liste de surveillance.

II. Le fonctionnement et l'expansion des différents systèmes d'information européens

51.- Eurodac – Eurodac est une base de données utilisée par 32 pays dont les 28 Etats membres de l'Union européenne, instituée par les Règlements 2725/2000[110] et 407/2002[111]. Ce système d'information permet de mettre en œuvre le Règlement de Dublin permettant de vérifier si le demandeur a déjà demandé l'asile et déterminer quel Etat membre est responsable de l'examen d'une demande d'asile. Cette base de données contient des données à caractère personnel, certaines sensibles, d'individu âgés de plus de 14 ans[112] : empreintes digitales, sexe, pays d'origine. Ces données sont conservées pendant dix ans ou jusqu'à l'obtention de la citoyenneté de l'Union européenne. En mai 2016, la Commission a fait une proposition de réforme[113] afin de collecter davantage de données à caractère personnel, dont les images faciales, d'étendre le champ d'application et de simplifier l'accès pour les autorités. Les autorités nationales qui examinent ou qui effectuent des enquêtes sur les demandes d'asile ont accès à ces données.

---

[110] Règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin

[111] Règlement (CE) n° 407/2002 du Conseil du 28 février 2002 fixant certaines modalités d'application du Règlement (CE) n°2725/2000 concernant la création du système Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin

[112] Rapport d'information n°898 des députés Ludovic MENDES et Christophe NAEGELEN, 19 avril 2018, *l'Espace Schengen et la maîtrise des frontières extérieures de l'Union européenne*

[113] Communiqué de presse du Conseil de l'Union européenne, « Réforme du régime d'asile européen commun : le Conseil est prêt à entamer des négociations sur Eurodac », 09 décembre 2016

52.- Système d'information sur les visas – Créé en 2004 et pleinement opérationnel dans tous les Etats membres depuis 2016, le système d'information sur les visas (VIS) est utilisé dans le cadre de la procédure de délivrance des visas de court séjour. Il est institué par le Règlement 67/2008[114] et la Décision 2004/515/CE[115]. Cette base est composée de bases de données telles que les empreintes digitales, photographies, l'identité du demandeur, les demandes antérieures, les demandes des personnes avec qui le demandeur a voyagé. Toutes ces données sont conservées pendant cinq ans et ne sont accessibles que par les autorités du pays qui a inséré ces données. Par un communiqué de presse[116], le Conseil de l'Union européenne a déclaré vouloir intégrer également les visas nationaux et les titres de séjour dans le VIS. En d'autres termes, le VIS pourrait à l'avenir contenir davantage de données à caractère personnel car plus de demandes et d'individus seraient alors concernés. Les autorités nationales qui examinent et mènent les évaluations quant aux contrôles relatifs aux visas Schengen aux frontières Schengen, les autorités qui étudient les demandent de protection dans le cadre d'une demande d'asile et EUROPOL d'une manière plus limitée ont accès à ces données.

53.- Bases de données Interpol – Interpol dispose de près de 19 bases de données mais l'ETIAS se réfère uniquement aux bases de données SLTD et TDAWN qui répertorient, à l'échelle internationale, tous les documents de voyage qui ont été volés, perdus ou révoqués, soit près de 99 millions de documents[117]. Chaque Etat, par le biais de son bureau central national Interpol, signale le document qui fait l'objet d'un signalement et y insère une copie de cette pièce.

54.- Système entrée/sortie – Institué par les Règlements 2017/2225[118] et 2017/226[119], le système entrée/sortie (EES) sera mis en application à compter de février 2022. Ce système[120] enregistre les données concernant les entrées, sorties et refus d'entrées des ressortissants de pays tiers, et pas uniquement pour ceux soumis à l'obligation d'obtention d'une autorisation de voyage. C'est donc un répertoire de tous les mouvements transfrontaliers en Europe dont les données sont conservées pendant cinq ans. Le nom,

[114] Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 09 juillet 2008 concernant le système d'information sur les visas et l'échange de données entre les Etats membres sur les visas de court séjour
[115] Décision 2004/512/CEdu Conseil du 08 juin 2004 portant création du système d'information sur les visas (VIS)
[116] Communiqué de presse du Conseil de l'Union européenne, « Système d'information sur les visas : accord provisoire entre la présidence du Conseil et le Parlement européen sur les points principaux », 08 décembre 2020
[117]https://www.interpol.int/fr/Notre-action/Bases-de-donnees/Base-de-donnees-sur-les-documents-de-voyage-voles-ou-perdus
[118] Règlement (UE) n° 2017/2225 du Parlement européen et du Conseil du 30 novembre 2017 en ce qui concerne l'utilisation du système entrée/sortie
[119] Règlement (UE) n° 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système entrée/sortie pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des Etats membres et portant détermination des conditions d'accès à l'EES à des fins répressives
[120]https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/securing-euborders/factsheets/docs/factsheet-entryexitsystemfr.pdf

les numéros de passeport, visa, empreintes digitales et photos sont les types de données à caractère personnel contenues dans l'EES. Or, le Code Schengen ne prévoit en aucun cas l'enregistrement de tous ces mouvements. En effet, il impose uniquement des vérifications approfondies des ressortissants des pays tiers et que les passeports soient tamponnés avec les dates d'entrée et de sortie[121]. Les garde-frontières et garde-côtes n'auront donc plus à rechercher mentalement si les dates d'entrée et de sortie correspondent à ce qui est autorisé par le Code frontières Schengen puisque le système entrée/sortie l'indiquera automatiquement. Cela a pour avantages[122] de fluidifier les flux aux points de vérifications aux frontières et de détecter plus aisément si la durée du séjour a été dépassée.

55.- Casiers judiciaires – Institué par les décisions-cadres 2009/315/JAI[123] et 2009/316/JAI[124], le système européen d'information sur les casiers judiciaires (ECRIS) permet aux Etats membres de l'Union européenne de partager des informations sur des condamnations prononcées à l'encontre de ressortissants de pays tiers ou de citoyens de l'Union ayant une ou plusieurs nationalités de pays tiers. Tous les Etats peuvent avoir accès aux informations concernant l'identité, le sexe, la date et lieu de naissance ainsi que des images faciales des individus présents sur cette base de données. Lorsqu'un Etat souhaite obtenir des informations sur les condamnations d'un individu en particulier, il doit faire une demande auprès de cet Etat qui a saisi ces données. Les données à caractères personnels sont conservées tant que les condamnations sont inscrites dans le casier judiciaire. Une réforme du système a été adoptée le 09 avril 2019[125] qui tend principalement à fluidifier les échanges d'informations pour une meilleure coopération entre les autorités des Etats membres.

56.- Liste de surveillance ETIAS – La liste de surveillance n'est pas un système européen d'information mais une base de données annexe à l'ETIAS. Les articles 34 et 35 du Règlement 2018/1240 sont relatifs à cette liste, qui va plus loin que le système ECRIS. En effet, cette liste répertorie de *« personnes soupçonnées d'avoir commis une infraction terroriste ou une autre infraction pénale grave ou d'y avoir participé, ou à des personnes pour lesquelles il existe des indices concrets ou des motifs raisonnables permettant de croire, sur la base d'une évaluation globale de la personne, qu'elles*

[121] F. GAZIN, « Frontières externes à l'Union européenne : principe des contrôles généralisés », *Répertoire de droit européen*, Janvier 2020

[122] https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/biometrie/systeme-entree-sortie

[123] Décision cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les Etats membres (ECRIS)

[124] Décision cadre 2009/316/JAI du 06 avril 2009 relative à la création du système européen d'information sur les casiers judiciaires (ECRIS)

[125] Règlement (UE) n° 2019/816 portant création d'un système centralisé permettant d'identifier les Etats membres les informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN)

commettront une infraction terroriste ou une autre infraction pénale grave »[126]. Ainsi, des personnes dont les autorités jugeraient qu'elles constituent une menace pour la sécurité européenne seraient sur cette liste, sans qu'elles n'aient été condamnées. Certes, des indices raisonnables doivent exister à leur encontre mais peut-on accepter le fichage de ces personnes sur des suppositions ? Cette liste de surveillance est établie grâce à la liste des criminels de guerre de l'ONU et d'informations fournies par les Etats membres de l'Union européenne ou grâce à la coopération internationale. Seuls les pays membres de l'espace Schengen auront accès à cette base de données. Europol est chargé de la gestion de cette liste et de sa sécurité.

57.- Une collecte d'informations grandissante – Il faut constater que de plus en plus de bases de données sont créées au nom de la sécurité publique, et qui vont au-delà de ce qui était originellement prévu par le Code frontières Schengen. Ces systèmes européens d'information tendent à s'étendre afin de collecter de plus en plus de données à caractère personnel. Cette collecte est multipliée par le développement de l'interopérabilité qui apparaît comme la solution aux problématiques actuelles.

Section II. L'effet multiplicateur de la mise en place de l'interopérabilité

58.- Définition – L'interopérabilité est la *« capacité de matériels, de logiciels différents à fonctionner ensemble et à partager des informations »*[127]. Ainsi, l'interopérabilité permet de mettre en connexion tous les systèmes d'information européens et d'obtenir l'information recherchée sans avoir à consulter chacun d'entre eux. Par ce mécanisme, les autorités disposent ainsi de données plus fiables et plus complètes, ce qui permet d'analyser de façon plus poussée l'éventuel risque que pourrait constituer un individu désirant entrer sur le territoire de l'espace Schengen. Cependant, cette architecture multiplie de manière importante le nombre de traitements de données à caractère personnel. En effet, un demandeur en déclinant uniquement son identité ou en donnant ses empreintes digitales, les autorités peuvent avoir accès à un historique complet sur l'individu si celui-ci fait l'objet de divers signalements.

59.- Cadre légal – L'article 11 du Règlement prévoit l'interopérabilité entre le système ETIAS et les autres systèmes d'information de l'Union européenne. C'est grâce à cette disposition que le système ETIAS est capable de faire toutes les vérifications nécessaires afin de délivrer une autorisation de voyage à un individu. Plus largement, l'interopérabilité entre toutes les bases de données est une initiative récente puisqu'elle

[126] Article 34 Règlement n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[127] Dictionnaire Larousse, 1996

est instituée le 14 mai 2019, par l'adoption des Règlement 2019/817[128] et 2019/818[129]. Ces deux textes couvrent l'ensemble des systèmes d'information européens ainsi que les bases de données d'Europol. L'interopérabilité est ainsi applicable depuis le 11 juin 2019.

60.- Fonctionnement et objectifs de l'ESP – De nouveaux éléments techniques sont donc mis en place pour centraliser l'ensemble des renseignements de l'Union européenne. Le principal est le portail de recherche européen (*European Search Portal*), l'ESP, qui permettra d'interroger l'ensemble des systèmes d'information européens ainsi que les bases de données en se basant sur des informations liées à l'identité de l'individu. Il n'y aura aucun stockage de données à caractère personnel dans l'ESP puisqu'elles seront recherchées directement dans les différentes bases de données européennes et ne ressortiront que les informations nécessaires. Ce portail permettra un accès moins fastidieux et plus fiable aux renseignements recherchés mais surtout d'améliorer l'identification d'une personne. Ainsi, un individu enregistré dans plusieurs systèmes d'information européens pourrait être reconnu avec un seul élément technologique. Pour ce faire, le portail de recherche européen est composé[130] d'une infrastructure centrale qui permet de faire la recherche dans les systèmes européens d'informations, ainsi que les bases de données d'Europol et Interpol. Puis, d'un canal de communication qui permet la transmission sécurisée de données entre le portail et les Etats membres ou les agences européennes autorisées, c'est-à-dire celles qui ont accès à au moins un système d'information de l'Union.

61.- Corrélation entre information et sécurité – Cette collecte boulimique de données à caractère personnel se révèle être une réelle mesure compensatoire[131] des problématiques relatives aux contrôles des frontières extérieures de l'Union européenne. L'interopérabilité de données de plus en plus importantes mais surtout de plus en plus sensibles est brandie par les institutions de l'Union européenne comme étant la solution à la crise actuelle, ce qui *de facto* crée une forte attente quant aux résultats de cette architecture. Ainsi, la sécurité des frontières de l'espace Schengen ne reposerait que sur l'existence tant quantitative que qualitative de données à caractère personnelles. Certains auteurs, tel que qu'Henri Labayle[132], considèrent que ce développement numérique, en plus d'être bien trop rapide pour les Etats, pourrait causer une baisse de leur vigilance

[128] Règlement (UE) n° 2019/817 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union Européenne dans le domaine des frontières et des visas
[129] Règlement (UE) n° 2019/818 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union Européenne dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration
[130] Article 6 et 7 du Règlement (UE) n° 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas
[131] E. Brouwer, "Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information System", Leiden, *Martius Nijhoff Publishers*, 2008
[132] H. Labayle, « Schengen, un coupable idéal », *GDR*, 25 novembre 2015

dans leur mission de surveillance des frontières. Cependant, l'efficience de l'interopérabilité et plus largement de l'utilisation de tous ces systèmes d'information européens repose sur la capacité des Etats à être rigoureux sur d'une part l'introduction complète de signalements et d'autre part sur le fait de consulter et de coopérer avec les autres partenaires en présence d'un individu qui présenterait un éventuel risque de sécurité ou sanitaire. En outre, le principe de confiance mutuelle est au cœur du fonctionnement de ces systèmes d'information. En effet, pour prendre une décision sur un individu, chaque Etat doit faire confiance à son partenaire sur la qualité des données. Il s'agit donc d'un partage de souveraineté entre les pays utilisateurs de ces bases.

Chapitre II. Le rôle central et renforcé de l'agence européenne eu-LISA dans la gestion des données à caractère personnel

L'agence européenne eu-LISA qui occupe une position centrale dans la gestion des systèmes d'information européens s'est vu octroyer des missions de plus en plus élargies (I) impliquant un accroissement de sa responsabilité (II)

Section I. Le poids prépondérant de l'agence eu-LISA par l'élargissement de son mandat

L'agence européenne eu-LISA mise en place en 2011 (I) a connu un élargissement de son mandat en 2017 grâce à ses résultats jugés satisfaisants (II).

I. La mise en place de l'agence européenne eu-LISA

62.- Création d'une nouvelle agence européenne- L'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'Espace de liberté, de sécurité et de justice, communément appelée eu-LISA, a été créée en 2011 par le Règlement 1077/2011[133] et est dotée de la personnalité juridique[134]. Eu-LISA a commencé son activité dès le 01 décembre 2012 avec la gestion du VIS. Son siège se trouve à Tallinn, en Estonie, mais puisque la gestion opérationnelle du SIS II et du VIS était effectuée à Strasbourg, en France, et dans une proportion plus limitée à Sankt Johann im Pongau en Autriche, il a été décidé de maintenir le centre opérationnel en France et l'unité de secours en Autriche[135]. Initialement, les tâches de conception et de développement techniques des systèmes d'information étaient confiées à la Commission européenne qui les a transférées à cette agence européenne. Cependant, la Commission encadre son fonctionnement. Eu-LISA travaille en étroite collaboration avec les Etats membres et les autres agences européennes, en particulier l'agence européenne chargée de la sécurité des réseaux et de l'information (AESRI).

63.- Missions initiales – Après avoir confié la gestion opérationnelle du SIS II, une actualisation du Règlement créant Eu-LISA a confié à l'agence européenne l'administration du VIS ainsi qu'Eurodac[136]. Dès le début, les institutions européennes

[133] Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

[134] Article 10 paragraphe 1 et 2 du Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

[135] J. MOLINIER, « Les Agences de l'Union européenne », *Revue du droit européen*, 2011

[136] Article 1 paragraphe 2 du Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

ont eu cependant des ambitions plus importantes pour cette agence puisqu'il est clairement mentionné dans l'article 1 paragraphe 3 et l'article 6[137] que *« l'agence peut également être chargée de la conception, du développement et de la gestion opérationnelle de systèmes d'information à grande échelle autres que ceux visés au paragraphe 2 (..) en tenant compte le cas échéant des progrès de la recherche ».* Afin d'assurer un suivi constant, le centre opérationnel fonctionne en continu 7 jours par semaine et 24 heures par jour. En effet, les agents qui y travaillent doivent s'assurer que l'ensemble des systèmes d'information, dont ils ont la charge, fonctionnent de manière efficace, qu'un niveau élevé de sécurité soit assuré en ce qui concerne les données et que l'unité de communication qui permet la transmission des signalements et des données soit opérationnelle.

64.- Présence des Etats membres – Forte de son expérience avec l'établissement de l'agence FRONTEX, l'objectif de la Commission européenne fut de donner un plein pouvoir à l'agence Eu-LISA afin que celle-ci puisse être effective tel que souhaité dans son Règlement de création, et ce sans que la réticence des Etats membres puisse faire obstacle à ses missions. Ainsi, un conseil d'administration, composé d'un représentant de chaque Etat membre et de deux de la Commission européenne siègent afin de valider les actions et le budget nécessaire à l'agence[138]. Les Etats disposent également d'un droit de véto. Ce fonctionnement s'avère être aujourd'hui efficient.

II. L'élargissement de son mandat en 2017 à la vue de ses résultats satisfaisants

65.- Des résultats encourageants – La Commission européenne a effectué une évaluation sur les actions menées par l'agence Eu-LISA de décembre 2012 à septembre 2015, conformément à l'article 31 paragraphe 1 du Règlement l'instituant[139]. Dans son rapport[140] établi en juin 2017, la Commission considère que *« l'agence eu-LISA contribuait efficacement à la création d'un environnement informatique plus coordonné, efficace et cohérent pour la gestion de systèmes d'information à grande échelle facilitant la mise en œuvre des politiques dans le domaine de la justice et des affaires intérieures »*

[137] Article 1 paragraphe 3 et article 6 du Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

[138] Article 11 à 16 du Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

[139] Article 31 paragraphe 1 du Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

[140] Rapport de la Commission au Parlement européen et au Conseil du 29 juin 2017 sur le fonctionnement de l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA)

et que *« la création de l'agence eu-LISA a apporté une valeur ajoutée, notamment en réunissant les trois systèmes « sous un même toit »*. Bien que certaines lacunes, nécessitant des réajustements, aient été révélées, l'évaluation de l'agence s'avère être positive. En effet, la Commission envisage d'étendre les missions confiées à l'agence européenne, dès avril 2016[141].

66.- Une assistance auprès des Etats – En vue de l'élargissement du mandat de l'agence eu-LISA, la Commission européenne a déposé une proposition en ce sens en juin 2017[142]. Les institutions, qui misent sur l'interopérabilité et accessoirement sur la bonne coopération des Etats membres, souhaitent qu'eu-LISA encadre les Etats membres. Ainsi, il est proposé qu'eu-LISA puisse fournir un accompagnement et des recommandations aux Etats concernant l'interconnexion des systèmes nationaux aux systèmes d'information européens. Cette assistance pourrait également s'étendre à la Commission dans une moindre mesure. Dans cette même démarche de collaboration, la Commission permettrait à l'agence de développer d'autres systèmes d'information si au moins six Etats membres le souhaitent. Il apparaît clairement que la création de nouveaux systèmes n'est pas une idée enterrée.

67.- De nouveaux systèmes d'information à charge – L'une des propositions capitales est l'élargissement du mandat afin que l'agence puisse gérer les récents systèmes d'information, à savoir l'ETIAS, l'EES et l'ECRIS. Pour ce faire, le budget a été revu à la hausse (78 millions d'euros supplémentaires) et un recrutement de personnel a eu lieu.

68.- La consécration en 2018 – Les institutions européennes ont adopté en 2018 un nouveau Règlement[143] qui abroge l'ancien Règlement de 2011 qui instituait l'agence eu-LISA. Les deux principales propositions de la Commission européenne ont été retenues. Désormais, eu-LISA est chargée de la gestion opérationnelle du SIS II, VIS, Eurodac, de la préparation en vue du développement de l'EES, l'ETIAS et ECRIS, d'apporter assistance aux pays de l'Union européenne et à la Commission et de mettre en place toutes les mesures nécessaires à l'efficience de l'interopérabilité de tous ces systèmes. À la vue de l'ampleur des missions confiées à l'agence, il peut être opportun de s'interroger sur sa responsabilité quant à la protection des droits fondamentaux.

---

[141] Communication de la Commission au Parlement européen et au Conseil, « Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité », 06 avril 2016,

[142] Proposition de Règlement du Parlement européen et du Conseil du 29 juin 2017 relatif à l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

[143] Règlement (UE) n° 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA)

Section II. La responsabilité *de facto* croissante à l'égard des droits fondamentaux

69.- Une responsabilité à relativiser – En effectuant une analyse peu approfondie des différentes bases légales qui instituent les différents systèmes d'information européens dont l'agence a la charge et celle qui crée l'agence, il pourrait apparaître qu'eu-LISA effectue des traitements de données à caractère personnel de manière importante. Cependant, cette analyse est erronée. En effet, l'agence a un rôle purement technique sur ces systèmes d'information puisqu'elle ne gère que la partie opérationnelle. Certes, un flux important de données à caractère personnel est transmis entre les Etats membres dont l'agence assure l'effectivité mais à aucun moment eu-LISA, qui est le sous-traitant, n'a connaissance de la teneur de ces données ou les manipule. Les données à caractère personnel qui sont traitées par les unités centrales sont fournies et utilisées uniquement par les autorités des Etats membres. L'agence est *« responsable des mesures techniques nécessaire à l'accomplissement des tâches qui lui sont confiées, qui n'ont pas de caractère normatif »*[144]. La responsabilité de l'agence quant à une potentielle violation des droits fondamentaux est donc à relativiser. Cet argument est confirmé par la Commission européenne qui considère qu'elle *« élargit la portée des tâches et des responsabilités de l'Agence, notamment en confiant à celle-ci de nouveaux systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice. Toutefois, son incidence sur les droits fondamentaux est limitée »*[145]. Cependant, l'une des nouvelles missions confiées à eu-LISA remettrait en cause cette responsabilité amoindrie.

70.- Ses nouvelles missions quant à la qualité des données – Dans le nouveau Règlement adopté en 2018, l'agence eu-LISA doit mettre en place des *« mécanismes automatisés de contrôle de la qualité des données et d'indicateurs communs de qualité des données, ainsi qu'à l'élaboration d'un répertoire central des rapports et statistiques »*[146]. Cette nouvelle fonction a pour objectif de mettre en évidence les données qui seraient erronées afin que l'autorité nationale qui les a fournies puisse apporter une correction si nécessaire[147]. Le répertoire commun est donc créé à cet effet et permet d'obtenir des statistiques fiables. L'article 12 du Règlement mentionne que ce répertoire

[144] Règlement (UE) n° 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA)

[145] Proposition de Règlement du Parlement européen et du Conseil du 29 juin 2017 relatif à l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

[146] Article 12 du Règlement (UE) n° 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA)

[147] P. BERTHELET, « L'Agence de sécurité des réseaux est une agence « performante » et « de plus en plus importante »,06 septembre 2017

ne peut contenir *« que des données anonymisées »*. Cependant, à quel stade du processus le sont-elles ? Pour que l'autorité nationale puisse vérifier et corriger la donnée à caractère personnel qui est problématique, celle-ci a besoin d'éléments clairs. Ainsi, l'agence aurait donc un accès à la teneur des données à caractère personnel contenues dans les systèmes d'information européens. Cette nouvelle activité est-elle donc autorisée ? Quelles garanties sont mises en place pour le droit à la protection des données à caractère personnel ? Cette nouvelle tâche crée une responsabilité incontestable de l'agence à l'égard des droits fondamentaux, même s'il est vrai qu'elle reste limitée. Eu-LISA a nommé en 2018 un délégué à la protection des données à caractère personnel. Il fait notamment le lien entre l'agence et le Comité européen de la protection des données qui *« supervise le traitement des données à caractère personnel de l'agence »*[148].

[148] https://www.eulisa.europa.eu/Activities/Data-Protection/Data-Protection-Officer

Partie II - LES ENJEUX DU DROIT À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL FACE AUX NOUVEAUX BESOINS DE SÉCURITÉ ET D'INFORMATION

La discutabilité de l'effectivité du droit à la protection des données à caractère personnel (I) révèle l'équilibre cornélien mais politique entre protection et sécurité (II).

Titre I- La discutabilité de l'effectivité du droit à la protection des données à caractère personnel

De grands principes et droits à la protection des données ont été proclamés progressivement (I) mais ils sont aujourd'hui confrontés à une ingérence au nom de la sécurité publique (II).

Chapitre I. L'évolution des grands principes du droit à la protection des données à caractère personnel

Des principes relatifs au traitement de données à caractère personnel (I) et des droits ont été proclamés progressivement aux individus concernés (II).

Section I. Les principes attachés au traitement des données à caractère personnel

Avant de d'étudier les principes qui découlent du Règlement Général sur la Protection des Données (II), il est nécessaire de démontrer que la construction du droit à la protection des données s'est faite en plusieurs étapes (I).

I. L'historique de la réglementation relative aux données à caractère personnel

Trois étapes peuvent être distinguées dans le processus de construction du droit à la protection des données à caractère personnel : des initiatives dans les années 1970 (A), une harmonisation à partir de 1995 (B) et une consécration dès 2016 (C).

A. Des initiatives dès les années 1970

71.- Projet SAFARI – Le 21 mars 1974, le journal Le Monde titre « SAFARI ou la chasse aux français »[149]. Le dévoilement du projet gouvernemental Système Automatisé pour les

[149], P. BOUCHER, « Une division de l'informatique est créée à la chancellerie « Safari » ou la chasse aux Français », *Archive le Monde*, 21 mars 1974

Fichiers Administratifs et le Répertoire des Individus, dit SAFARI, crée un scandale au sein de la population française ce qui oblige Pierre Messmer, le Premier Ministre, d'abandonner le projet. Ce projet consistait en la création de fichiers, qui permettaient l'identification des Français à partir de leur numéro de sécurité sociale, et dans lesquels toutes les informations détenues par les différents pouvoirs publics pouvaient être stockées[150]. Par ce projet, le gouvernement a souhaité fluidifier et accélérer la circulation des données. Cette affaire a pris une telle ampleur que le gouvernement a créé une Commission « Informatique et Libertés » avec pour objectif d'étudier le traitement informatique des données et proposer des moyens pour l'encadrer.

72.- Loi Informatique et Libertés – La Commission rend le 08 novembre 1974 son rapport[151] dit Tricot, qui s'avère être capital puisqu'il constituera la base de la loi Informatique et Libertés[152] du 06 janvier 1978. Cette loi est fondatrice du droit à la protection des données à caractère personnel. A la date de sa promulgation, seuls les fichiers étaient visés.

73.- A l'échelle européenne – La question du traitement des données à caractère personnel ne s'est pas uniquement posée à l'échelle nationale. En effet, en 1980, le Conseil de l'Organisation de Coopération et de Développement Economiques (ci-après « OCDE ») a publié des recommandations à propos de la protection des données dans le cadre des flux transfrontières[153]. Souhaitant avoir un niveau élevé de protection, le Conseil de l'Europe a adopté une convention[154] en la matière l'année suivante.

B. L'harmonisation à partir de 1995

74.- Création d'un socle commun – Les institutions européennes en 1995 souhaitent harmoniser la législation en vigueur en ce qui concerne le traitement de données personnelles. Ainsi, en 1995, la Directive 95/46[155] reprend les principes présents dans la loi de 1978. Tous les Etats membres doivent avoir une législation sur le sujet et créer une autorité administrative indépendante.

---

150 MOOC créé par la CNIL, *Atelier RGPD*, 2021

151 Rapport de la Commission informatique et liberté, *La documentation française*, décret n°74.938 du 08 novembre 1974

152 Loi n°78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

153 Recommandation du Conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, 23 septembre 1980

154 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, n°108, Conseil de l'Europe, 28 janvier 1981

155 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 2995, 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

75.- Réforme en 2004 – Au regard de l'avancement technologique et des usages numériques qui prennent une place plus importante, la loi Informatique et Libertés est amendée dans ce sens[156]. Les fichiers informatisés et le secteur privé sont désormais concernés par les dispositions de cette loi. Le rôle de l'autorité administrative indépendante et certains droits aux personnes sont étendus.

76.- A l'échelle européenne – L'article 8 de la Charte des droits fondamentaux de l'Union européenne[157] crée une nouvelle base légale en affirmant que « Toute personne a droit la protection des données à caractère personnel la concernant. ». En outre, le TFUE est modifié en 2007 par le Traité de Lisbonne dans lequel le nouvel article 16 garantit également cette protection.

C. La consécration depuis 2016

77.- Une consécration en 2016 – *« Les révélations d'Edouard Snowden nourrissent la prise de conscience collective sur la nécessité de revoir à la hausse le niveau de protection accordée aux données personnelles »*[158]. L'affaire Snowden a eu un retentissement mondial en 2013[159]. En effet, Edouard Snowden, anciennement agent de la Central Intelligence Agency (ci-après « CIA »), a alerté les médias sur l'existence d'un espionnage à grande échelle, mis en place par la National Security Agency (ci-après « NSA ») grâce à internet et aux téléphones portables. Les institutions européennes ont fortement condamné[160] ces agissements en les qualifiant *« d'atteintes graves au droits fondamentaux des citoyens européens »*. La naissance du Règlement Général sur la Protection des Données est clairement causée par cet évènement majeur qui a fait prendre conscience aux institutions européennes du risque réel sur les droits et les libertés des individus que constitue une telle profusion des données personnelles et la surveillance possible des personnes concernées grâce à celles-ci.

78.- De nouveaux textes législatifs - Sur le plan national, la loi pour une République numérique[161] enrichit la loi Informatique et Libertés et renforce les droits des personnes. Mais c'est sur le plan européen que la consécration de cette construction du droit à la protection des données à caractère personnel s'effectue : l'adoption du Règlement

[156] Loi n°2004-801 du 06 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
[157] Article 8 de la Charte des droits fondamentaux de l'Union européenne, du 18 décembre 2000
[158] F. MATTATIA, « RGPD et droit des données personnelles », 4e édition, paru en septembre 2019
[159] G. Greenwald, *"*NSA collecting phone records of millions of Verizon customers daily*", The Guardian,* 06 Juin 2013
[160] Communication de la Commission européenne au Parlement européen et au Conseil du 27 novembre 2013, « Rétablir la confiance dans les flux de données entre l'Union européenne et les Etats-Unis d'Amérique »
[161] Loi n°2016-1321 du 07 octobre 2016 pour une République numérique

Général sur la Protection des Données[162] le 27 avril 2016. L'adoption de ce texte abroge la Directive de 1995 mais plusieurs principes y sont repris. Les Etats membres ont un délai de 2 ans pour se conformer aux nouvelles dispositions. Il est transposé en droit interne par une loi promulguée en 2018[163]. Le RGPD n'abroge pas la loi Informatique et Libertés, toujours en vigueur.

II. Les principes fondamentaux relatifs au traitement des données à caractère personnel

A. Définition du traitement de données et champ d'application du RGPD

79.- Définitions – Le RGPD définit une donnée à caractère personnel comme étant *« toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une personne physique identifiable une personne physique qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant, tels qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »*[164]. Quant au traitement de données à caractère personnel, il s'agit de *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, telle que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »*[165].

80.- Champ d'application – Le RGPD est applicable à tous les organismes publics ou privés établis sur le territoire de l'un des Etats membres (critère de l'établissement) ou dont l'activité cible des personnes qui se trouvent sur le territoire de l'Union européenne (critère de ciblage)[166]. L'organisme peut être responsable de traitement tout comme pour

---

[162] Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[163] Loi n°2018-494 du 20 juin 2018 relative à la protection des données personnelles

[164] Article 4 paragraphe 1 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[165] Article 4 paragraphe 2 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[166] Articles 2 et 3 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

son éventuel sous-traitant s'il traite des données. En revanche, le RGPD ne s'applique pas aux traitements qui sont réalisés pour un usage strictement personnel : l'exception domestique[167].

B. Les principes de la protection des données

Les principes quant au traitement des données sont attachés à sa licéité (1), sa finalité (2), sa minimisation (3), sa conservation et sa sécurité (4). Un traitement spécifique est réservé aux données dites sensibles (5).

1. Licéité du traitement

81.- Fondée sur l'une des six conditions– La CJUE considère que tout traitement de données à caractère personnel par un tiers constitue une atteinte au droit et au respect de la vie privée ainsi qu'au droit à la protection des données personnelles[168]. Ainsi, pour que le traitement de données à caractère personnel soit licite, il doit être fondé sur l'une des six bases autorisant ce traitement :

> *« - la personne concernée a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques ;*
> *- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;*
> *- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis ;*
> *- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ;*
> *- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement ;*
> *- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par un tiers à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. »*[169]

[167] MOOC, *Atelier RGPD,* CNIL, 2021
[168] CJUE, Michael Schwarz c/ Stadt Bochum, 17 octobre 2014, affaire C-291/12, paragraphe 24 et 25
[169] Article 6 paragraphe 1 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

82.- Consentement de l'individu – Le RGPD définit le consentement comme étant *« toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »*[170]. Cette condition préfigurait déjà dans la loi Informatique et Libertés. Le RGPD précise la notion afin de s'assurer que la personne effectue un réel choix. Des conditions supplémentaires sont posées pour les mineurs puisque ceux de moins de 15 ans ne peuvent consentir au traitement de leur données[171]. Le responsable de traitement doit être capable de prouver que le consentement de la personne était libre, éclairé, univoque et spécifique[172]. Un registre des activités de traitement doit être mis en place afin de documenter la conformité et recenser tous les traitements opérés par l'entreprise[173].

83.- Exécution d'une mission d'intérêt public – Cette base ne peut être utilisée que par une autorité publique ou un organisme privé doté de prérogative de puissance publique. Le traitement de données à caractère personnel ne peut concerner que les usages et non le personnel. Enfin, l'intérêt public doit être défini par une base légale, qu'elle soit française ou européenne.[174] La mission d'intérêt public ne peut cependant pas avoir lieu à l'étranger.

2. Finalité du traitement

84.- Principe – Les données à caractère personnel collectés ne peuvent être traitées que s'il existe une finalité définie et légitime, c'est-à-dire que l'usage des données doit être délimité avec un objectif déterminé. Il est interdit de traiter des données personnelles pour toutes fins utiles. A défaut, le RGPD considère cela comme un détournement de finalité qui est sanctionné pénalement[175] et administrativement[176]. En cas d'évolution de l'usage

[170] Article 4 paragraphe 11 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[171] Considérant 38 et article 8 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[172] Article 7 paragraphe 1 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[173] Article 30 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[174] https://www.cnil.fr/fr/la-mission-dinteret-public-dans-quels-cas-fonder-un-traitement-sur-cette-base-legale

[175] Article 226-21 du Code pénal

[176] Article 83-5 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

des données, cette finalité devra être compatible avec la première. Le RGPD prévoit 3 finalités[177] qui sont par principe compatibles et détermine une méthode de faisceaux d'indices[178]. Si la nouvelle finalité n'est pas compatible alors il est considéré qu'il s'agit d'un nouvel usage. Le responsable de traitement devra alors obtenir à nouveau le consentement des personnes ou faire signer un autre contrat.

3. Minimisation des données

85.- Minimisation des données – Seules les données strictement nécessaires pour atteindre l'objectif déterminé peuvent être collectées et traitées[179]. Dès la conception d'un projet, le responsable de traitement doit donc choisir et pouvoir justifier les données utilisées pour atteindre la finalité. Son objectif est de traiter le moins possible de données personnelles, sur un temps déterminé, tout en atteignant l'objectif fixé. Le recours à l'anonymisation permet de respecter ce principe tout en traitant des données personnelles.

4. Conservation limitée et sécuritaire des données

86.- Temps de conservation des données – Dès que la finalité définie est atteinte, les données doivent être archivées, supprimées ou anonymisées. Il n'est pas possible de traiter des données pendant une durée illimitée. Ainsi, le responsable de traitement doit préalablement définir une durée de conservation ou un critère qui détermine cette durée. La loi définit dans certains cas la durée pendant laquelle les données doivent être conservées. La CNIL distingue trois phases : la conservation en base active ; l'archivage intermédiaire et l'archivage définitif. Pour la première, la durée doit être égale à la durée nécessaire à l'accomplissement de la finalité. L'archivage intermédiaire doit remplir des conditions supplémentaires pour permettre une durée de conservation plus longue. Une séparation distincte doit avoir lieu entre les données de la première et seconde phase. La seule exception à la conservation limitée dans le temps est l'archivage définitif. Cela est possible uniquement s'il existe un intérêt public, historique, scientifique ou statistique.

87.- Conservation sécurisée des données – Le responsable de traitement et le sous-traitant éventuel doivent prendre toutes les mesures nécessaires afin d'assurer un niveau

[177] Article 5 paragraphe 1 alinéa b du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[178] Article 5 paragraphe 1 alinéa b du Règlement (CE) n° d2016/679 u Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[179] Article 5 paragraphe 1 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

élevé de sécurité des données personnelles traitées. Quatre principes en découlent[180] : le principe de confidentialité ; le principe d'intégrité ; le principe de disponibilité ; le principe de traçabilité. Le principe de confidentialité implique que seules les personnes autorisées peuvent accéder à ces données, ce nombre droit être limité au stricte nécessaire. Le chiffrement des données ou la pseudonymisation permettent par exemple de garantir la confidentialité des données contenues dans le fichier. C'est au responsable d'apprécier le risque et de mettre en œuvre les mesures nécessaires. Le principe d'intégrité permet aux données ne pas être modifiées à l'insu de l'individu. Enfin, le principe de disponibilité signifie que les données doivent être accessibles. Au-delà des données, le responsable de traitement et le sous-traitant doivent également protéger les locaux qui hébergent ces données.

5. Protection particulière des données sensibles

88.- Des conditions plus restrictives – Ces données sont dites sensibles d'un point de vue des libertés et des droits fondamentaux. Les données sensibles font référence au numéro de sécurité sociale, aux condamnations pénales, aux données relatives à l'opinion politique, à la santé ou encore aux donnés génétiques et biométriques. Le RGPD prohibe par principe le traitement de ces données[181]. Des exceptions sont cependant possibles et sont encadrées par le RGPD[182]. Pour permettre le traitement de ces données, le responsable de traitement devra obligatoirement justifier la base légale de son traitement ainsi que son exception. Le consentement de la personne est l'une de ces exceptions mais celui-ci devra être explicite. En ce qui concerne les données personnelles relatives aux condamnations, elles ne peuvent être traitées que par les juridictions, autorités publiques, les personnes physiques ou morales pour la défense de leurs intérêts. La Directive 2016/680 encadre ce traitement spécifique *« par les autorités compétentes dans le domaine de la prévention et la détection des infractions pénales, les enquêtes et poursuites en la matière ainsi que l'exécution de sanctions pénales y compris la protection contre les menaces pour la sécurité publique, la prévention de telles menaces et la libre circulation de ces données »*[183]. Le RGPD et cette Directive, dite Police-Justice

[180] Article 32 paragraphe 1 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[181] Article 9 paragraphe 1 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[182] Article 9 paragraphe 2 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[183] Article 1 de la 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 poursuite en la matière ou l'exécution de sanction pénales, et à la libre circulation de ces données

composent *« le paquet européen relatif à la protection des données à caractère personnel »*. Les principes posés par le RGPD sont repris dans cette Directive. Il exige également que soit distinguées les données personnelles relatives à des personnes où des raisons raisonnables portent à croire qu'elles sont sur le point de commettre une infraction pénale, les personnes reconnues coupables et les victimes d'infractions. Il est nécessaire de mettre en avant que le Comité Européen de la Protection des Données (ci-après « CEPD ») a rendu un avis défavorable[184] sur l'autorisation du traitement de ces données notamment à l'égard de personnes présumées innocentes jusqu'à ce que leur culpabilité soit démontrée[185]. L'article 34 de la Directive 2016/680 autorise ce traitement qu'en cas de *« nécessité absolue »* et que des garanties soient accordées. Catherine FORGET, avocate au barreau de Bruxelles, considère *« qu'il est regrettable que les droits des personnes concernées n'aient pas été davantage affirmés et soient amputés d'exceptions* »[186]. En effet, les personnes concernées possèdent des droits identiques à ceux conférés par le RGPD.

Section II. Les droits des individus concernés et l'autorégulation

Le RGPD prévoit des droits hautement protecteurs pour les individus (I) dont certaines autorités nationales et européennes en sont les gardiennes (II).

I. Les droits hautement protecteurs pour les individus à l'égard de leurs données à caractère personnel

Quatre grands droits ont été consentis à l'égard des individus et de leurs données à caractère personnel : le droit d'information (A), le droit d'accès et de rectification (B), le droit d'opposition (C) et le droit à l'oubli (D).

A. Droit d'information

89.- Principe de loyauté et de transparence – Un principe de loyauté et de transparence est imposé par le RGPD vis-à-vis des individus concernés par le traitement de leurs données. Avant un quelconque traitement, plusieurs informations doivent être communiquées aux intéressés. En effet, les individus doivent connaître ce qui justifie la collecte des données, comprendre les conditions dans lesquelles leurs données sont traitées et être informés de leur droit d'accès, de rectification, d'opposition, d'effacement

[184] CEPD, avis n°6/2015, 2015
[185] Article 6 de la Convention européenne des droits de l'Homme du 04 novembre 1950
[186] C. FORGET, « Protection des données dans le secteur de la « police » et de la « justice » », Février 2019

et au droit à la portabilité des données[187]. Cette obligation exige que les données soit recueillies directement ou indirectement auprès des individus. Dans le cas d'une collecte directe, le responsable de traitement doit également fournir l'identité et les coordonnées de l'organisme responsable, le caractère obligatoire ou non de la collecte, le destinataire de ces données ou encore la durée de conservation.

B. Droit d'accès et rectification

90.- Droit d'accès – Toute personne dont les données à caractère personnel sont traitées ont un droit d'accès conformément à l'article 15 du RGPD[188]. Cela implique qu'il lui est possible à tout moment d'exiger du responsable de traitement qu'il lui communique toutes les données la concernant, l'informer sur la durée de conservation, les destinataires de ces données. Le responsable de traitement doit au préalable s'assurer de l'identité du demandeur. En effet, aucune communication sur les données personnelles d'une personne autre que le demandeur ne peut avoir lieu, y compris le conjoint de la personne concernée. Le droit d'accès peut concerner toutes les données relatives à la personne ou encore des données plus spécifiques ou sur une période en particulier. S'agissant d'une demande simple, le responsable de traitement a une obligation de répondre sous un mois maximum, sauf en cas de demande complexe où le délai est porté à 3 mois. Une exception relative aux données de santé impose une communication sous 8 jours maximum. Ce droit s'exerce gratuitement mais il est possible de faire supporter au demandeur des frais dits *« raisonnables basés sur les coûts administratifs »*[189]. En outre, le RGPD impose également que *« les informations [soient] fournies sous une forme électronique d'usage courant »*[190] en d'autres termes sous la forme d'un document clair et lisible.

91.- Droit à la rectification – Le droit à la rectification permet à l'individu concerné de corriger ou de compléter le contenu de ses données si celles-ci sont inexactes ou ne sont plus d'actualité[191]. Le responsable de traitement est alors tenu de procéder aux corrections

[187] Article 12 à 14 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[188] Article 15 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[189] Article 15 paragraphe 3 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[190] Article 15 paragraphe 3 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[191] Article 16 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

« dans les plus brefs délais ». Ce droit peut être limité pour certains fichiers, en particulier ceux de police ou de renseignement.

C. Droit d'opposition

92.- Retrait du consentement – Le droit d'opposition est la possibilité de refuser, même après acceptation, que les données personnelles de l'individu puissent être traitées[192]. En revanche, cela ne signifie pas une suppression des données puisqu'il s'agit d'une opposition et non d'un retrait du consentement. La personne concernée devra invoquer les motifs qui justifient son opposition, ce droit est donc conditionné. Ainsi, le droit d'opposition peut être limité s'il existe *« des motifs légitimes et impérieux »* à ce traitement, une obligation légale ou si le traitement est motivé *« à la sauvegarde des intérêts vitaux de la personne »*. Pourtant, en 1995, il était prévu initialement que ce droit pourrait s'exercer de manière discrétionnaire sans aucun motif légitime[193]. Ce conditionnement est cependant à relativiser car la Cour de cassation adopte une appréciation large en considérant qu'en *« matière politique, philosophique ou religieuse, la condition de l'existence de motif légitimes est remplie par le seul exercice de la faculté, pour la personne concernée, de s'opposer au traitement de données personnelles »*[194].

D. Droit à l'oubli

93.- Conséquence du principe de conservation limitée des données – Le droit à l'effacement, appelé également le droit à l'oubli, est la possibilité pour l'individu concerné d'effacer ses données, *« dans les meilleurs délais »*[195]. Cela est cependant possible si la demande est basée sur l'un des motifs prévus par le RGPD. En outre, ce droit est limité s'il existe une obligation légale, s'il existe un intérêt public ou encore dans l'exercice du droit à la liberté d'expression et d'information.

[192] Article 21 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[193] Groupe de travail « article 29 » sur la protection des données – Lignes directrices sur la transparence au sens du Règlement (UE) n° 2016/679 adoptées le 29 novembre 2017

[194] Cass. Crim. 28 septembre 2004 pourvoi n°03-86.604

[195] Article 17 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

II. L'existence d'autorités gardiennes du respect de ces droits

La Commission Nationale de l'Informatique et des Libertés à l'échelle nationale (A) et le contrôleur européen de la protection des données avec la Cour de Justice de l'Union européenne à l'échelle européenne (B) sont les autorités gardiennes des droits des personnes.

A. A l'échelle nationale : la Commission Nationale de l'Informatique et des Libertés

94.- Construction progressive – Proposition du rapport Tricot, la loi Informatique et Libertés de 1978 créée une autorité administrative indépendante de l'Etat, la CNIL. Ses prérogatives ont été étendues progressivement pour devenir une véritable autorité de régulation[196] qui atteint aujourd'hui son apogée avec la pandémie actuelle. La CJUE considère que cette autorité est indispensable pour le respect du droit à la protection des données personnelles[197]. Cette commission a initialement pour mission principale de rendre des avis sur les projets relatifs à des traitements de données à caractère personnel et de veiller au respect des droits accordés aux personnes concernées. En 2004, lors de la réforme, la CNIL est investie de pouvoirs de sanction et la fonction de Correspondant Informatique et Liberté (ci-après « CIL ») est créée. Ce dernier a pour rôle d'être l'intermédiaire entre la CNIL et les entreprises. Le RGPD a considérablement renforcé les pouvoirs de sanctions de l'autorité[198]. Avant 2018, le CIL devait effectuer des déclarations à la CNIL, sur la base de normes simplifiées, pour pouvoir autoriser l'entreprise à opérer des traitements de données personnelles. Ces anciennes normes permettaient, par exemple, le traitement de données qui concerne le contrôle des accès aux locaux de l'entreprise grâce à un badge (NS 42)[199] ou encore la mise en place d'écoute et d'enregistrement des conversations téléphoniques sur le lieu de travail (NS 57)[200]. Le RGPD a rendu ces normes obsolètes en opérant un renversement de la responsabilité. Désormais le délégué à la protection des données n'effectue plus de déclaration pour obtenir une autorisation de la CNIL. En vertu du principe d'accountability *(cf. paragraphe 95)*, l'entreprise prend la responsabilité quant à la conformité de ses traitements. En contrepartie de ce rapport de confiance, le montant de l'amende maximum est colossal et n'a cessé d'augmenter. La loi Informatique et Libertés fixait ce montant à 300 000 euros, puis la loi pour une République numérique l'a augmenté à 3 millions

[196] F. MATTATIA, « RGPD et droit des données personnelles », 4e édition,paru en septembre 2019
[197] CJUE, Schrems c/ Data Protection Commissionner of Ireland, 06 octobre 2015, affaire C-362/14 §41
[198] C. FERAL-SCHUHL, « Les règles générales, CNIL : une autorité de contrôle pour la France », *Cyberdroit*, Titre 11, 2019
[199] https://www.cnil.fr/sites/files/ns42.pdf
[200] https://www.cnil.fr/sites /files/ns57.pdf

d'euros pour atteindre 20 millions d'euros ou 4% du chiffre d'affaire annuel mondial en 2018[201].

95.- Missions de la CNIL - La CNIL aujourd'hui possède 4 grandes missions[202] : informer et protéger les droits qui sont garantis ; accompagner la conformité ; anticiper et animer le débat éthique ; contrôler et sanctionner.

96.- Informer et protéger les droits – En tant que garante des droits des individus, la CNIL reçoit toutes les réclamations des demandeurs qui souhaitent exercer leur droit mais qui soit n'ont pas eu de réponse, soit celle-ci leur était insatisfaisante. Depuis l'entrée en vigueur du RGPD, le nombre de réclamations est en constante augmentation. A titre d'exemple, la CNIL a reçu 14 137 réclamations en 2019, soit une hausse de 27%[203]. La prise de conscience sur les questions de protection des données personnelles est aussi due au travail important de communication qui est réalisé par la CNIL afin de sensibiliser et former la population sur ces enjeux.

97.- Accompagner la conformité – Le RGPD met en place le principe d'*accountability*[204] définit par la CNIL comme étant *« l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données »*[205]. La CNIL a pour mission de les accompagner afin de trouver les mesures adaptées et nécessaires. Elle avise également les autorités publiques sur leurs projets de textes. Les risques encourus en cas de non-respect de cette obligation sont importants. Les responsables de traitement doivent donc collaborer étroitement avec cette autorité nationale. L'utilisation accrue de nouvelles technologies et les menaces liées à la cybersécurité rendent le rôle de la CNIL central.

98.- Anticiper et animer le débat éthique – La CNIL a également pour objectif de susciter le débat au sein de notre société et de prévoir les enjeux de demain afin de mieux les appréhender. Le Laboratoire d'Innovation Numérique mis en place par la CNIL a cet objectif. Des missions ponctuelles peuvent aussi lui être confiées par le biais législatif. Ainsi, la loi pour une République numérique a associé la CNIL afin qu'un travail de réflexion soit effectué sur l'évolution des technologies numériques avec un débat très poussé sur l'intelligence artificielle. Une autre mission lui a été également confiée par la

[201] Article 83 paragraphe 5 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
[202] E. DELISLE, « Le nouveau rôle de la CNIL », *JS* 2019, n°196
[203] Le Monde, « Le nombre de plaintes à la CNIL en hausse de 27% en 2019 », publié le 09 juin 2020
[204] Responsabilité
[205] https://www.cnil.fr/fr/definition/accountability

loi relative à la lutte contre le terrorisme[206]. En effet, la CNIL opère un contrôle sur le blocage administratif des sites qui font l'apologie du terrorisme ou qui ont un caractère pédopornographique.

99.- Contrôler et sanctionner – La CNIL peut se rendre à tout moment et sans besoin de prévenir en amont, dans les locaux d'une entreprise, d'une association ou des autorités publiques afin de vérifier que l'ensemble des dispositions relatives au droit à la protection des données à caractère personnel soient bien appliquées. Si les mesures instaurées sont insatisfaisantes ou nulles, l'organisme sera mis en demeure de se conformer dans un délai donné. Afin d'assurer une pression efficace sur la réputation de l'organisme en cause[207], la CNIL peut décider de rendre publique sa décision. Diverses sanctions peuvent être infligées et permettent de dissuader les responsables de traitement.

100.- Affaire British Airways – « Lorsqu'on vous confie des données personnelles, vous devez les protéger. Ceux qui ne le feront pas seront poursuivis par l'ICO pour vérifier qu'ils ont pris les mesures adéquates »[208]. C'est dans ces termes que s'est exprimée la commissaire de l'*Information Commissioner's Office* (ci-après « ICO »), qui l'autorité de régulation au Royaume-Uni, à propos de l'affaire concernant British Airways en octobre 2020. La compagnie aérienne britannique a été épinglé par l'ICO pour la violation de son obligation de sécurité. En effet, le site web de la compagnie a été piraté ce qui a permis aux hackers d'avoir accès aux données personnelles, dont les coordonnées bancaires, de 430 000 passagers[209]. L'ICO a souligné la négligence du transporteur, quant à la sécurité de ces systèmes informatiques, en démontrant qu'il existe des moyens pour les rendre plus sures et que les mesures prises sont insuffisantes[210]. L'amende de près de 183 millions de livres sterling a été fixé en prenant compte *« la nature des données compromises », « la durée significative des violations »* et *« le nombre de personnes concernées »*. Cependant des circonstances atténuantes telle que la coopération de l'entreprise et l'existence de mesures prises pour remédier rapidement au manquement constaté a permis de diminuer l'amende à 20 millions de livre sterling[211] ; ce qui demeure conséquent notamment au regard de l'impact de la pandémie de la Covid-19 sur le secteur aérien. Cette affaire démontre également la nécessité de coopération des autorités européennes de régulation lorsque la violation des données personnelles concerne des

[206] Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme
[207] C. FERAL-SCHUHL, « Les règles générales, CNIL : une autorité de contrôle pour la France », *Cyberdroit,* Titre 11, 2019
[208] Le Monde, « 204 millions d'euros d'amende pour British Airways après un vol massif de données bancaires de ses clients », publié le 08 juillet 2019
[209]https://www.alain-bensoussan.com/avocats/cybersecuriteetrgpddeux-amendes-records-au-royaumeuni/2020/11/17/
[210] ICO Penalty Notice, British Airways, case ref. COM0783542, 16 october 2020
[211]https://www.alain-bensoussan.com/avocats/cybersecurite-et-rgpd-deux-amendes-records-au-royaume-uni/2020/11/17/

individus de nationalités différentes. Le RGPD a pris en compte ces cas de figure en exigeant la désignation d'une seule autorité de contrôle par pays comme l'interlocuteur principal et en imposant la reconnaissance dans toute l'Union européenne d'une décision émise par l'une de ces autorités[212].

B. A l'échelle européenne : le Contrôleur européen de la protection des données et la Cour de Justice de l'Union européenne

1. Le Comité européen de la protection des données

101.- Avant 2018 – Le groupe de travail « article 29 » sur la protection des données est le prédécesseur du comité européen de la protection des données, qui a été institué par la Directive de 1995[213]. Organe européen consultatif indépendant, il était composé de toutes les autorités nationales de régulation et du contrôleur européen à la protection des données et de la Commission européenne.

102.- Créé par le RGPD – Le RGPD a remplacé le G29 par le CEPD, tout en gardant la même composition. Ce comité ne doit pas être confondu avec le contrôleur européen de la protection des données[214] qui est une autorité européenne de contrôle qui veille au respect du droit de la protection des données à caractère personnel au sein des institutions de l'Union. Alors que le CEPD veille à ce que ce droit soit appliqué au sein de l'Union. Cette autorité à l'échelle européenne est importante afin d'avoir une harmonisation tant sur l'application et l'interprétation du texte entre les Etats membres. Ainsi, le CEPD coordonne les actions menées en rendant des avis et des décisions, publie des lignes directrices et conseille la Commission européenne pour toute question qui attrait à la protection des données à caractère personnel. Il peut également être saisi pour les litiges qui concerne des traitements de données transfrontalières.

2. La Cour de Justice de l'Union européenne

103.- L'autorité judiciaire à l'échelle européenne – La Cour de Justice de l'Union européenne donne les interprétations relatives à la législation européenne et en conséquence du RGPD. Ces décisions sont juridiquement contraignantes puisque les institutions de l'Union et les Etats membres doivent les suivre. Elle veille également à

[212] Articles 56 à 60 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
[213] Article 29 et 30 de 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
[214] https://edps.europa.eu/_fr

l'existence d'une indépendance réelle des autorités de contrôles nationales puisqu'un contrôle strict est effectué par la CJUE[215].

[215] CJCE, Commission des communautés européennes / République fédérale d'Allemagne, 09 mars 2010, affaire c-518/0

« Quoi de plus paradoxal que d'observer au moment où une nouvelle législation européenne dite « RGPD » protège les données personnelles, l'apparition d'une autre le 20 mai 2019 qui organise l'ouverture des fichiers relatifs aux migrants portés par les Etats, au nom de la sécurisation du territoire de l'Union. »[216]

Loïc GRARD

Chapitre II. Des principes et des droits confrontés à une ingérence au nom de la sécurité publique

De grands principes ont été érigés progressivement par l'Union européenne mais sont aujourd'hui confrontés au traitement de données au nom de l'exécution d'une mission d'intérêt public (I) ayant pour principale conséquence un déséquilibre notable entre les individus concernés et les différentes autorités nationales et européennes (II).

Section I. La particularité d'un traitement de données au nom de l'exécution d'une mission d'intérêt public

Il est nécessaire d'étudier la particularité de ce traitement de données en s'attachant au principes (I) afin de pouvoir discuter de l'ingérence qui est effectuée au nom d'une notion floue et mal définie (II).

I. L'étude du respect des principes attachés au traitement de données

104.- Bases légales – D'après le Règlement instituant l'ETIAS[217], le RGPD est applicable pour le traitement de données effectués par les unités nationales, EUROPOL, les autorités frontalières, celles désignées par les Etats et celles chargées de l'immigration. La Directive 2016/680 s'applique également pour le traitement de données des condamnations pénales et toutes informations liées aux infractions et enquêtes. FRONTEX est le responsable de traitement des données dans le système ETIAS et l'agence eu-LISA le sous-traitant, à l'exception de la gestion de la sécurité où cette dernière est la responsable de traitement[218].

---

[216] L. GRARD, « Protection des données personnelles des migrants et fermeture des frontières de l'Union européenne », *Revue de l'Union européenne*, 04 septembre 2020

[217] Article 56 du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

[218] Article 57 et 58 du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

105.- Licéité du traitement – Le traitement de données à caractère personnel dans le système central d'ETIAS est bien basé sur l'une des six conditions puisqu'il « *est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement* ». Le traitement est opéré par plusieurs autorités publiques, nationales et européenne, afin de veiller à la sécurité et aux contrôles des frontières extérieures de l'espace Schengen. Il concerne bien les usagers puisque les données personnelles traitées sont celle des demandeurs d'une autorisation de voyage qui souhaitent venir sur le territoire de l'espace Schengen. Par conséquent, le traitement de données personnelles est licite au sens du RGPD.

106.- Finalité du traitement - En ce qui concerne la finalité du traitement, la CJUE considère que la lutte contre l'entrée illégale d'individus sur le territoire de l'Union européenne constitue un *« objectif d'intérêt général reconnu par l'Union »* qui permet de limiter l'exercice du droit à la protection des données à caractère personnel[219]. La sécurité publique est également considérée comme étant un *objectif d'intérêt général* permettant des restrictions qui ne doivent cependant pas être disproportionnées ou injustifiées[220]. Le traitement de données personnelles dans le système ETIAS a pour but d'assurer un niveau élevé de sécurité et de lutter contre l'immigration illégale ou de personnes qui constituent un risque. En ce qui concerne l'interopérabilité des systèmes d'information européens, il est regrettable qu'aucune finalité n'ait été définie. En effet, chaque système possède une finalité propre mais l'interopérabilité fait disparaitre les causes de la collecte de données.

107.- Conservation limitée des données - Les données personnelles sont conservées dans le système central ETIAS *« pendant la durée de validité de l'autorisation de voyage »* ou *« cinq ans à compter de la dernière décision de refus, d'annulation ou de révocation de l'autorisation de voyage »*[221]. Une conservation plus longue de trois années supplémentaires peut avoir lieu mais uniquement si le demandeur y consent par une déclaration. Une durée de conservation a donc bien été établie mais celle-ci doit intervenir lorsque la finalité définie est atteinte. Il est concevable que la conservation des données s'achève à la fin de la durée de validité de l'autorisation de voyageur. Le demandeur ne peut plus accéder au territoire de l'espace Schengen au-delà de cette période. Il n'est donc plus nécessaire de s'assurer que l'individu constitue un risque sanitaire et d'ordre public. Cependant, la seconde durée pose davantage question. En effet, la finalité est-elle atteinte au bout de ces cinq années ? Sur quel critère est-elle basée ? Les motifs du refus, de l'annulation ou de la révocation d'une autorisation de voyage sont certes importantes mais

[219] CJUE, Michael Schwarz / Stadt Bochum, 17 octobre 2013, affaire C-291/12
[220] CJUE, Digital Rights Ireland / Steitlinger, 08 avril 2014, affaire C-293/12 et C-594/12
[221] Article 54 du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

elles peuvent l'être de manière indéfinie. Il apparaît donc que cette durée de conservation soit basée sur des considérations plus approximatives et floues. Aucun archivage intermédiaire, sauf consentement de l'individu concernée et archivage définitif ne sont prévus par les textes. Il faut néanmoins noter que ces durées ne concernent que le système central de l'ETIAS et non celles des autres systèmes d'information de l'Union. En effet, EURODAC a fixé une durée de conservation des données pendant dix ans[222], le VIS l'a fixé à cinq ans et l'EES pendant trois ans. Ainsi, les données à caractère personnel peuvent être supprimées dans l'ETIAS sans que cela ne soit le cas dans les autres bases de données et systèmes d'information européens.

108.- Conservation sécurisée des données – L'agence eu-LISA, l'unité centrale et les unités nationales doivent avoir un plan de sécurité et de continuité des activités en cas de défaillance du système[223]. Ces deux plans sont adoptés par la Commission européenne qui n'a pour l'heure pas encore communiqué leurs contenus. Le Règlement instituant l'ETIAS affirme que *« l'accès à celles-ci* - le système central ETIAS - *devrait être limité au personnel strictement autorisé. (…) Les données à caractère personnel qui sont conservées devraient l'être de manière sécurisée dans les installations de l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice »*[224]. En cas d'incident, l'autorité ou l'agence européenne concernée est tenue de prévenir la Commission, l'agence eu-LISA et le contrôleur européen de la protection des données dans les plus brefs délais. Si l'incident est majeur au regard du risque que cela pourrait constituer, les demandeurs doivent être avertis. Un régime de responsabilité est également institué entre l'agence eu-LISA et les Etats membres, permettant ainsi de sanctionner en cas de défaillance ou de violation des mesures prises pour assurer la sécurité des données et réparer en cas de dommage.

109.- Protection particulière des données sensibles – La Directive 2016/680 est également applicable aux données personnelles contenues dans le système central ETIAS relatives aux condamnations pénales, enquêtes en cours. Le Règlement instituant l'ETIAS ne prévoit aucune mesure, garantie supplémentaire que celles prévus par la Directive et le RGPD. Ce manque de protection peut être reproché compte tenues du volume des données personnelles traité et de l'interopérabilité avec plusieurs systèmes qui multiplient

[222] Article 6 du Règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin
[223] Article 59 du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[224] Considérant 30 du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

considérablement les opérations de traitement d'autant plus que les autorités nationales peuvent se communiquer ces données sensibles.

II. Une ingérence possible au nom de notions floues

110.- Une notion laissant une marge d'interprétation – L'intérêt général est défini par Cornu comme étant *« ce qui est pour le bien public »*[225]. Le Conseil d'Etat donne deux conceptions différentes pour tenter de définir cette notion : *« Deux conceptions de l'intérêt général s'affrontent. L'une, d'inspiration utilitariste, ne voit dans l'intérêt commun que la somme des intérêts particuliers, laquelle se déduit spontanément de la recherche de leur utilité par les agents économique, cette approche non seulement laisse peu de place à l'arbitrage de la puissance publique mais traduit une méfiance envers l'Etat. L'autre conception, d'essence volontariste (…) exige le dépassement des intérêts particuliers [et] est d'abord dans cette perspective l'expression de la volonté générale, ce qui confère à l'Etat la mission de poursuivre des fins qui s'imposent à l'ensemble des individus, par-delà leurs intérêts particuliers »*[226]. La volonté générale souhaite-t-elle réellement que les données à caractère personnel des individus soient traitées à outrance jusqu'à ne plus en avoir un contrôle réel ? L'Etat ne voudrait-il pas plutôt préserver l'ordre public, dont il est responsable, mais étant lui-même dépassé dans ses missions n'a plus d'autre choix que d'imposer des contrôles plus poussés, même si cette intrusion implique une ingérence dans le droit à la protection des données personnelles pourtant de plus en plus affirmé depuis cinquante ans ? Les décisions des dirigeants européens ne sont-elles pas la conséquence de pressions politiques notamment de certains partis extrémistes et la montée de l'europhobie ? L'intérêt général et l'ordre public sont des notions floues qui par conséquent laissent une marge d'appréciation importante[227]. Cornu considère que l'ordre public est *« un ensemble de principes, écrits ou non, qui sont, au moment même où l'on raisonne, considérés dans un ordre juridique, comme fondamentaux et qui, pour cette raison imposent d'écarter l'effet dans cet ordre juridique non seulement de la volonté privée mais aussi des lois étrangères et des actes des autorités étrangères »*[228]. Plusieurs auteurs mettent en avant l'impuissance de l'Etat à encadrer la collecte et le flux importants de données personnelles, quitte à lui-même les utiliser pour mettre en œuvre ses prérogatives[229]. Certains pourront donc considérer que tel est le cas dans la mise en œuvre de l'ETIAS mais bien plus largement dans ce besoin et cette attente forte qu'ont les institutions de l'Union européenne dans la mise en œuvre

[225] Vocabulaire juridique, Gérard Cornu, 13e édition, Association Henri Captant
[226] Rapport public du Conseil d'Etat, Réflexions sur l'intérêt général 1999
[227] J. GHESTIN, « L'ordre public, notion à contenu variable », p. 77
[228] Vocabulaire juridique, Gérard Cornu, 13e édition, Association Henri Captant
[229] A. DANIS-FATOME, « Ordre public et protection des données à caractère personnel », 18 septembre 2019

de l'interopérabilité. D'autres considèreront que les Etats s'adaptent et utilisent les moyens numériques de notre temps afin de protéger les frontières de l'espace Schengen. Le but principal est-il seulement la protection de ces frontières qui posent tant de problématiques ou bien les dirigeants souhaitent-ils avoir des renseignements plus poussés sur les individus présents sur leur territoire ? Cette ingérence des autorités publiques crée incontestablement un déséquilibre entre les individus concernés et elles. Pour rappel, les individus entrants sont des étrangers de l'Union européenne. Quelle est la légitimité de l'Union à porter atteinte à leurs droits ?

> *« Etant donné que ces moyens supposent souvent le traitement de volumes importants de données à caractère personnel, il convient d'instaurer des garanties appropriées afin de limiter l'ingérence vis à vis du droit à la protection de la vie privée et du droit à la protection des données à caractère personnel à ce qui est nécessaire dans une société démocratique. »*[230]

Section II. Le déséquilibre notable entre les individus et autorités nationales et européennes

Le déséquilibre entre les individus et les autorités se démontre par l'impossibilité d'avoir un traitement données personnelles basé sur le consentement réel du demandeur (I) et par une architecture trop complexe pour le demandeur qui indubitablement restreint leurs droits (II).

I. L'obtention impossible d'un consentement réel

111.- Un consentement qui peut difficilement avoir lieu – La pierre angulaire du traitement de données à caractère personnel est le consentement. C'est d'ailleurs sur cette condition que la majorité des traitements de données se font. Comme étudié précédemment, le RGPD exige que le consentement de l'individu concerné soit *« libre, spécifique, éclairé et univoque »*. La mise en place de l'ETIAS ne peut se fonder sur ce principe car le conditionnement du traitement par le consentement réel de l'individu ferait défaut, mettant ainsi en échec le but recherché. En effet, le terme libre signifie que le consentement ne doit subir aucune conséquence en cas de refus. Ce refus en aurait puisque l'autorisation de voyage serait refusée au demandeur. Un consentement spécifique doit correspondre à l'acceptation d'une seule finalité déterminée. En cas de plusieurs finalités,

[230] Considérant 29 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

l'individu doit consentir à toutes celles-ci, indépendamment. En admettant que le demandeur d'une autorisation de voyage accepte la finalité de l'ETIAS, il devrait alors accepter la finalité de tous les systèmes d'information européens et de l'interopérabilité qui n'est pas déterminée. Cela paraît difficilement envisageable. Le consentement doit également être éclairé c'est-à-dire que toutes les informations doivent être distinctement communiquées et qu'elles puissent être consultables facilement. Au vu du caractère complexe du mécanisme mis en œuvre, le demandeur risque en plus d'être noyé dans un flot d'informations et être incapable de déchiffrer toutes les données. En effet, des compétences nécessaires sont essentielles afin de décrypter les nombreux textes législatifs nationaux et européens pour s'assurer que le demandeur puisse avoir un consentement réellement éclairé. Le Règlement instituant l'ETIAS prévoit une information à destination du grand public notamment via le site internet qui va être mis en place prochainement, ainsi qu'une campagne d'information afin de faire connaître l'ETIAS et ses modalités[231]. Ces renseignements seront donnés dans *« au moins une des langues officielles des pays dont les ressortissants relèvent »*. Pour parfaire cette volonté d'éclaircissement, il aurait été également souhaitable de faire de la pédagogie sur l'interopérabilité qui est au cœur du système d'ETIAS. Ce manquement d'information et son impossibilité au regard de la complexité sur le mécanisme permet d'affirmer qu'un consentement éclairé n'aurait pu être faisable. Enfin, ce consentement doit être univoque c'est-à-dire donné sans aucune ambiguïté, soit par une déclaration soit par un acte positif. La CJUE a rappelé récemment qu'une case pré-cochée avant l'acceptation ne peut être considérée comme permettant l'obtention d'un consentement univoque[232]. Le système ETIAS conserve les données à caractère personnel au-delà de la durée de conservation uniquement si le demandeur y consent. Cela s'effectue grâce à une déclaration en ligne. L'impossibilité d'obtention d'un consentement réel dans un tel cadre est également mise en avant par la CJUE dans une affaire similaire où le requérant s'opposait au prélèvement de ses empreintes digitales pour l'obtention d'un passeport : *« En ce qui concerne, tout d'abord, la condition tenant au consentement des demandeurs de passeport avec le prélèvement de leurs empreintes digitales, il convient de relever que la possession d'un passeport est, en règle générale, indispensable aux citoyens de l'Union notamment pour effectuer des déplacements à destination de pays tiers et que ce document doit contenir des empreintes digitales (...). Ainsi, les citoyens de l'Union souhaitant effectuer de tels déplacements ne peuvent s'opposer librement au traitement de leurs empreintes digitales. Dans ces conditions, les demandeurs de passeports ne sauraient être considérés comme ayant consenti à un tel traitement »*[233]. L'obtention d'une autorisation de voyage peut également être

[231] Chapitre XIII du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[232] CJUE, Orange Romania SA c/ ANSPDCP, 11 novembre 2020, affaire C-61/19
[233] CJUE, Michael Schwarz c/ Stadt Bochum, 17 octobre 2013, affaire C-291/12, §32

indispensable pour certains ressortissants de pays tiers non soumis à l'obligation de visa. Le caractère nécessaire d'un tel document rend incompatible un consentement sincère créant indubitablement un déséquilibre entre les parties. En effet, cela signifie que l'autorité publique est assez puissante pour pouvoir imposer un traitement sans consentement. En outre, l'architecture construite autour du système ETIAS vient restreindre les droits d'étrangers de l'Union au nom de « *l'objectif d'intérêt général de l'Union européenne* ».

II. Une architecture complexe restreignant les droits des personnes

112.- Barrière de la langue – Le site internet et l'application qui vont être mis en place pour effectuer la demande seront *« dans toutes les langues officielles des Etats membres »*[234] et non dans les langues maternelles des étrangers qui peuvent donc être différente. Un premier obstacle peut être donc souligné dans la compréhension réelle des informations communiquées par les plateformes pour ces ressortissants. On peut également regretter l'absence de précision dans le Règlement instituant l'ETIAS de la nature des informations qui seront communiquées : *« les demandeurs dont les données sont conservées dans le système central ETAIS sont informés, au moment de la collecte de leurs données, des procédures à suivre pour exercer les droits prévus par les articles 15 à 18 du Règlement (UE) n°2016/679. Les coordonnées du délégué à la protection des données de l'Agence européenne de garde-frontière et de garde-côtes et du Contrôleur européen de la protection des données leurs sont également fournies dans le même temps »*[235]. Maîtriser l'une des langues des Etats membres ne signifie pas être capable de comprendre ces notions juridiques pouvant être abstraites, au regard de la complexité de l'architecture du système de l'ETIAS mais aussi du système législatif propre à l'Union européenne. Ces différentes barrières peuvent constituer une réelle difficulté et rendre l'obligation d'information et de transparence du responsable de traitement moins efficiente.

113.- A l'épreuve du temps et de la distance – Certains auteurs tel que Maxime Kheloufi mettent en avant une difficulté relative au temps dont dispose les demandeurs afin d'exercer leurs droits : *« Le temps juridique nécessaire pour l'exercice des droits prévus semble inadapté au phénomène migratoire et au rythme bien plus rapide qu'il implique »*[236]. Combien de demandeurs seront dissuadés par le délai de traitement de leur

[234] Article 16 paragraphe 3 du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[235] Article 64 paragraphe 1 du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)
[236] M. KHELOUFI, « Le droit à la protection des données à caractère personnel face au défi migratoire », *Revue de l'Union européenne*, 04 septembre 2020

demande, fixé à un mois pour les demandes simples et de trois mois pour les demandes plus complexes, et par le fait qu'ils ne se trouveront sans doute plus sur le territoire de l'espace Schengen à la réception d'une réponse ? En outre, après réception d'un traitement, combien de demandeurs s'aventureront dans des procédures judiciaires ou auprès d'une autorité de régulation nationale ou européenne à distance et sans connaître leur fonctionnement ? Toutes ces interrogations portent à croire que l'exercice des droits de ces ressortissants est restreint par toutes ces difficultés, malgré les nombreuses dispositions du Règlement affirmant l'existence de recours effectif pour garantir leurs droits.

114.- Droit de rectification – Le droit de rectification de ses données à caractère personnel est respecté, au sens du RGPD. En effet, l'unité centrale ou nationale modifie dans les plus brefs délais les données qui apparaitraient être inexactes ou qui auraient été enregistrées de manière illicite[237]. Aucune rectification n'est possible en dehors de ces deux cas de figure. Dans un tel cas, une lettre motivée est adressée au demandeur pour justifier le refus de modification de leurs données dans le système d'information.

[237] Article 55 et article 64 paragraphes 2 à 4 du Règlement (UE) n° 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

Titre II- Un équilibre cornélien mais politique entre protection et sécurité

Le difficile équilibre entre protection et sécurité se démontre par les exemples du Canada et des Etats Unis qui adoptent des philosophies diamétralement opposées (I). L'Europe fait le choix de protéger en optant pour le développement d'outils numériques mis au service de la sécurité (II).

Chapitre I. Entre approche économique et protectrice : les exemples étrangers

Le système américain a une approche économique (I) tandis que le Canada fait le choix de la protection (II).

Section I. Le système américain : une approche économique

Les Etats-Unis possèdent également une autorisation de voyage similaire à l'ETIAS (I). Cependant, la politique américaine de protection des données personnelles est davantage une politique de marché (II).

I. Le fonctionnement de l'autorisation électronique de voyage américaine

115.- Nécessité d'un visa ou d'un *Electronic System Travel Authorization* – Comme pour les Etats membres de l'espace Schengen, afin d'entrer aux Etats-Unis il est impératif de posséder soit un visa soit une autorisation de voyage, appelée ESTA. L'ESTA, à l'instar de l'ETIAS, permet d'évaluer le risque que constitue un demandeur et de posséder des informations sur lui, même si l'analyse est moins approfondie que celle effectuée lors d'une demande de visa. Les personnes qui ont la nationalité canadienne ou américaine sont les seules catégories de voyageurs qui n'ont pas besoin de tels documents. Un visa est nécessaire pour les situations suivantes[238] :

« - un séjour de plus de 90 jours consécutifs aux Etats-Unis ;
- si le motif du séjour n'est pas touristique, professionnel ou médical ;
- si un voyage a été effectué en Iran, Irak, Corée du Nord, Syrie, Soudan, Yémen, Libye ou Somalie depuis 2011 ;
- si le demandeur a la nationalité de l'un de ces pays ;
- si au moins une réponse est « non » aux questions posées dans le formulaire ESTA ;

[238] https://demandevisa.fr/etats-unis/visa

- si le demandeur ne peut rentrer dans le pays sur le fondement de l'Immigration and Nationaly Act §212 ;

- si le demandeur ne possède pas de passeport d'un pays qui participe au programme d'exemption de visa »

En dehors de toutes ces situations, le demandeur a tout intérêt à faire une demande d'ESTA. Il existe 185 visas différents aux Etats-Unis. Le demandeur doit choisir par lui-même lequel correspond au mieux à sa situation. Afin de promouvoir *l'american dream*, chaque année le Congrès américain organise une loterie, *The Green card lottery*, durant laquelle 50 000 green card sont gagnées par des étrangers.

116.- Electronic System for Travel Authorisation (ESTA) – Obligatoire depuis le 12 janvier 2009, l'ESTA, qui remplace l'ancien formulaire I-94W, s'effectue exclusivement en ligne. Les autorités chargées de l'immigration doivent apporter une réponse en moins de 72 heures mais il est possible de demander un ESTA en urgence où une réponse est apportée dans l'heure qui suit la demande. *Le Department of Homeland Security* gère le programme d'exemption de visa (Visa Wever program) qui répertorie tous les Etats dont les ressortissants peuvent entrer sur le territoire américain avec ce document. Ces pays sont principalement ceux d'Europe et d'Asie du Sud-Est où les autorités américaines considèrent qu'il y a un faible risque migratoire et sanitaire. L'ESTA est valable pendant deux ans pour un séjour de moins de 90 jours ou jusqu'à l'expiration du passeport et peut être utilisé pour plusieurs entrées. Contrairement à l'ETIAS, la demande d'ESTA peut être effectuée par une tierce personne. Les demandeurs doivent s'acquitter des frais de traitement qui s'élèvent à 14 USD. A l'embarquement, un portail pour les transporteurs aérien appelé APIS (système avancé d'information des passagers) permet d'autoriser ou non les passagers à monter à bord. Quel que soit le dossier, la détention d'un ESTA ne garantit pas automatiquement l'entrée sur le territoire des Etats-Unis. En effet, les agents des services de douane et d'immigration peuvent légalement refuser l'accès à un voyageur possédant cette autorisation de voyage. Tout comme l'ETIAS, l'ESTA corrobore les informations données par le demandeur avec de nombreuses bases de données fédérales et étatiques. L'interopérabilité est *a fortiori* moins importante qu'en Europe où les données sont partagées, voir communiquées entre tous les Etats membres de l'espace Schengen.

II. Régime américain de protection des données : les données personnelles comme biens marchands

117.- Droit à la protection de la vie privée – Le 4^{e} amendement section 4 de la Constitution des Etats-Unis, du 17 septembre 1787, exige du gouvernement, uniquement,

qu'il respecte la vie privée de ses concitoyens et aux étrangers vivant sur le sol américain. Ce principe est confirmé par la Cour suprême des Etats-Unis[239]. A l'inverse, l'Union européenne reconnaît ce droit comme étant universel et s'applique par conséquent également aux étrangers ne vivant pas sur le sol européen. En outre, ce droit s'impose aux autorités publiques mais également aux personnes et organismes privés. Samuel Warren et Louis Brandeis, juristes américains, ont publié *« The Right to Privacy »*[240] qui constitue les règles de responsabilité civile en ce qui concerne la vie privée, tel que l'article 9 du Code civil français.

118.- Encadrement du traitement de données par les FIPs – Le *Privacy Act*[241] de 1974 est le premier texte au niveau fédéral relatif à la protection des données à caractère personnel à l'égard de traitement effectué par le gouvernement fédéral. Cette loi érige des principes considérés comme équitables en matière de données, appelés également Fair information Practice (FIPs)[242]. Il existe cinq FIPs : interdiction des systèmes secrets d'enregistrement des données ; possibilité d'accès pour l'individu à ces informations ; principe de limitation de la finalité ; possibilité de rectification des informations et principe de sécurité des informations. Ces principes se retrouvent également dans le droit, tant français qu'européen, relatif à la protection des données à caractère personnel. Ce texte n'est cependant pas applicable aux citoyens non américains ou ne vivant pas aux Etats-Unis[243]. En outre, les requérants doivent, pour agir, justifier d'un préjudice et que les autorités publiques ont agi de manière intentionnelle ou délibérée à leur égard, ce qui limite de manière conséquent la possibilité d'un recours[244].

119.- Développement de lois sectorielles pour les acteurs privées – Aux Etats-Unis, il n'existe pas d'unique législation relative à la protection des données. En effet, pour les acteurs privés, plusieurs lois sont érigées en fonction du secteur d'activité. Ainsi, les règles sont hétérogènes. Pour exemple le *Health Insurance Portability and Accountability Act* vise à protéger les données relatives à la santé, le *Electronic Communications Privacy Act*, aux données rattachées aux télécommunications ou encore *le Children's Online Privacy Protection Act* relatif aux données concernant les mineurs.

120.- Affaire Snowden - Cette affaire met en lumière l'absence de protection à l'égard des citoyens non américains ou ne vivant pas sur le territoire, mais également la

[239] Supreme Court of the United States, Schmerber v. Californie, 20 juin 1966
[240] S. WARREN and L. BRANDEIS, "The Right to Privacy", 1890
[241] https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf
[242] W. J. MAXWELL, « La protection des données à caractère personnel aux Etats-Unis : convergences et divergences avec l'approche européenne »
[243] Privacy Act de 1974, §552a
[244] R. Bellanova et P. DE HERT, « Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique », 2009

surveillance de certains pays européens, telle que la France. Le Parlement européen a décidé l'arrêt immédiat de la sphère de sécurité[245], appelé le Safe Harbour, instituée par la Directive de 1995.

121.- Transfert des données entre l'Union européenne et des pays tiers – Le Safe Harbour interdit la possibilité de transférer des données à caractère personnel à des Etats tiers qui possèderait un niveau inférieur, en termes de protection des données personnelles, à celui de l'espace économique européen[246]. Cela impose à la Commission européenne d'effectuer un suivi constant des évolutions des politiques de protection des données personnelles dans tous les pays du monde, pour évaluer si l'Etat tiers possède un niveau de protection jugé adéquat aux normes européennes[247]. Le transfert de données hors Union européenne peut aussi être effectué en vertu de clauses contractuelles ou de règles d'entreprises internes[248].

122.- Vision commerciale des données personnelles – W. MAXWELL considère que *« l'une des plus grandes différences entre l'approche européenne et l'approche américaine concerne le caractère commercial ou non des données à caractère personnel »*[249]. En effet, aux Etats-Unis, il existe effectivement des lois sectorielles mais qui sont très spécifiques et constituent en réalité des exceptions. Les entreprises et personnes physique peuvent exploiter comme bon leur semble les données à caractère personnel. La donnée devient un bien marchand et prend de la valeur, il est possible de la marchander. La seule limite posée est la pratique déloyale. Cette vision n'est absolument pas partagée en Europe qui a érigé le droit à la protection des données comme fondamental et où aucun traitement de données par un tiers ou non autorisé n'est possible. Alex Turk, président de la CNIL, a résumé cet état de fait en expliquant qu'il *« y a un fossé abyssal entre la conception américaine des données personnelles qui sont pour eux des biens marchands et la conception européenne où il s'agit d'attribut de nos personnalités »*[250]. Cette vision s'explicite par le libéralisme très poussé pratiqué par les Etats-Unis.

---

[245] Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures

[246] Article 45 du Règlement (CE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[247] Article 2 de la Décision d'exécution (UE) 2016/2296 de la Commission européenne du 16 décembre 2016 constatant le niveau de protection adéquat des données à caractère personnel assuré par certains pays

[248] https://www.cnil.fr/fr/transferts-de-donnees-hors-ue-le-cadre-general-prevu-par-le-rgpd

[249] W. J. MAXWELL, « La protection des données à caractère personnel aux Etats-Unis : convergences et divergences avec l'approche européenne »

[250] A. NOIVILLE, « Valeur des données personnelles et protection des droits fondamentaux », octobre 2016

123.- Federal Trade Commission – La Federal Trade Commission est une agence fédérale dont l'indépendance pose question et qui a des compétences qui vont au-delà de la protection des données à caractère personnel. En effet, le but premier de cette autorité de régulation est la protection du consommateur. Les données à caractère personnel étant un bien, les individus deviennent par nature des consommateurs ou vendeurs. Telle que la CNIL mais de manière beaucoup moins poussée, la Federal Trade Commission doit informer le consommateur sur la collecte, l'utilisation et le partage de ses données personnelles. Seuls cinq types de comportement sont condamnés, à savoir les changements rétroactifs en matière de confidentialité, les pratiques pour installer des logiciels espions, l'utilisation inappropriée des données, la collecte illicite d'informations et les pratiques déloyales en matière de sécurité. Cependant, contrairement à la CNIL, la Federal Trade Commission a des pouvoirs très limités et n'a aucun moyen d'agir en cas de violation de ces principes. La seule sanction qui a abouti est celle infligée à Google en 2019 concernant les données personnelles des enfants[251].

124.- Vers des droits plus protecteurs ? – A la suite du scandale concernant Facebook Analytica[252], l'Etat de Californie a décidé d'imposer en 2020 grâce au *California Consumer Privacy Act* un droit d'information et de suppression des données collectées, tels que connus dans l'Union européenne. C'est une avancée majeure dans une philosophie diamétralement opposée aux européens qui faut cependant relativiser car les sanctions et les modalités d'application de celle-ci sont dérisoires. En outre, la Californie reste le seul Etat des Etats-Unis à avoir de telles dispositions ainsi qu'un département dédié à la protection de la vie privée[253].

125.- Un niveau de sécurité jugé non adéquat - L'Union européenne considère aujourd'hui que la politique américaine de protection des données à caractère personnel n'est pas satisfaisante au regard des normes européennes. Ainsi, la CJUE a annulé la décision de 2016 de la Commission européenne permettant le transfert de données personnelles vers les Etats-Unis[254].

[251]https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations

[252] Les données personnelles de 90 millions d'utilisateurs de Facebook ont été utilisé pour influencer les intentions de vote de plusieurs élections de 2014 à 2016

[253] I. JOLLY, "Data protection in United States: overview, practical law", 2014/2015, p.3

[254] CJUE, Data Protection Commissioner c/ Facebook Ireland and Maximillian Schrems, 16 juillet 2020, affaire C-311/18

Section II. Le système canadien : une approche protectrice

Tout comme l'Europe et les Etats-Unis, le Canada possède également une autorisation de voyage (I). La politique de protection des renseignements personnels est jugée adéquate aux normes européennes (II).

I. Le fonctionnement de l'autorisation électronique de voyage canadienne

126.- Conditions pour l'obtention d'un AVE – Obligatoire depuis novembre 2016, l'Autorisation de Voyage Electronique (AVE) canadien est nécessaire dans les conditions cumulatives suivantes :

« - Se rendre au Canada en avion ;
- Rester au Canada au maximum six mois consécutifs ;
- Le motif du séjour est touristique, professionnel ou il s'agit d'un transit aéroportuaire ;
- Disposer d'un titre de transport permettant de quitter à nouveau le pays ;
- Être ressortissant exempté de visa[255] *»*[256]

La différence notable avec l'ESTA ou l'ETIAS est que l'AVE est nécessaire uniquement si le ressortissant d'un pays tiers se rend au Canada par voie aérienne. L'AVE n'est pas nécessaire en cas d'entrée sur le territoire par bus, train, voiture, à pied ou en bateau. Les citoyens américains sont les seules catégories de voyageurs dispensés d'obtention d'une AVE ou d'un visa canadien. Les résidents permanents des Etats-Unis qui ne sont pas citoyens américains demeurent soumis à cette formalité. Tout comme les deux autorisations électroniques de voyage étudiées précédemment, la demande s'effectue exclusivement en ligne. Les demandeurs doivent s'acquitter des frais qui s'élèvent à 7$CAN. L'AVE est valable pendant cinq ans ou jusqu'à l'expiration du passeport et peut être utilisée pour des entrées multiples à condition de respecter la limite des six mois consécutifs. Il peut être remarqué que l'AVE contrairement à l'ETIAS et l'ESTA a des conditions moins strictes et une durée de validité plus longue. Les personnes qui ne remplissent pas les conditions pour entrer sur le territoire canadien avec une AVE doivent obligatoirement détenir un visa. Il en existe une dizaine qui peuvent être distingués en deux catégories : le visa de résident temporaire (*Temporary Resident Visa*) qui permet de faire des études, d'avoir des activités professionnelles ou être en vacances prolongées et le visa de résident permanent (*Permanent Resident Visa*) qui permet de s'installer durablement au Canada. Quand ce statut est acquis à vie, concernée sans preuve d'être resté sur le territoire pendant une période définie comme cela pour être le cas en France.

[255] La liste des Etats exemptés de visa Canadien : https://www.canada-ave.com/fr/visa
[256] https://www.canada.ca/fr.html

En août 2021, Justin Trudeau, Premier Ministre du Canada, a annoncé que seules les personnes vaccinées à la Covid-19 pourront entrer sur le territoire. Cette condition sera donc sans doute rajoutée dans le formulaire de l'AVE et les demandes de visa canadien. Cela s'appliquera également aux employés des compagnies aériennes[257].

127.- Vers une généralisation des autorisations électronique de voyage ? – En plus du Canada, des Etats-Unis et des Etats membres de l'espace Schengen, l'Australie a également mis en place un système d'autorisation électronique de voyage pour les ressortissants non soumis à l'obligation d'obtention d'un visa. Il serait sans doute trop tôt pour parler d'une généralisation de ces systèmes qui permettent de mieux contrôler les frontières de l'Etat grâce à l'interopérabilité. Cependant, les Etats et régions qui l'ont adopté sont des puissances influentes sur la scène internationale, qui connaissent des flux migratoires importants. Dans un monde qui doit faire face à de nouvelles menaces et où les populations se déplacent plus facilement qu'il y a quelques années, grâce à des mobilités devenues accessibles et plus performantes, il est possible d'envisager que d'autres Etats feront également le choix d'un tel système. Et cela d'autant plus que nombreux Etats acceptent l'entrée sur le territoire de ressortissants de pays tiers sans aucune formalité préalable. La question pendante est de connaître l'avenir des données à caractères personnels de ces futurs migrants. Le droit à la protection des données à caractère personnel est un sujet et une préoccupation d'actualité dans les pays démocratiques les plus développés mais des inégalités importantes persistent dans ce domaine en raison soit de l'obligation de priorisation de certaines problématiques soit par refus de donner un réel contrôle des données personnelles aux personnes concernées. Cela est le cas dans les pays dictatoriaux ou autoritaires.

II. Régime canadien de protection des renseignements : un niveau de protection adéquat aux normes européennes

128.- Charte canadienne des droits et des libertés – La Charte canadienne des droits et libertés est une loi fondamentale qui assure les droits fondamentaux des personnes, en vertu de la Constitution. De valeur supérieure, tous les textes législatifs doivent être promulgués dans le respect des dispositions de ce texte. L'article 8 de la Charte protège le droit à la vie privée, de manière universelle. Les citoyens non-canadiens ou ne vivant pas sur le territoire sont tout autant protégés puisque le Canada n'effectue pas la distinction faite par les Etats-Unis. Similaire au système juridique européen, les décisions

[257] S. FABI, « Canada : vaccination obligatoire pour les passagers et les employés des compagnies aériennes », *Air Journal*, le 14 août 2021

des tribunaux canadiens constituent des précédents qui sont contraignants et obligent les parties de s'y soumettre.

129.- Loi sur la protection des renseignements personnels et les documents électroniques – La loi sur la protection des renseignements personnels et les documents électroniques[258] (ci-après « LPRPDE ») a été adoptée au niveau fédéral le 13 avril 2000. Ce texte est applicable uniquement pour les traitements interprovinciaux ou internationaux. Mais il n'est pas applicable dans certaines provinces, comme au Québec, en Colombie-Britannique et en Alberta, qui disposent de règles propres.

130.- Loi sur la protection des renseignements personnels – La loi sur la protection des renseignements personnels est entrée en vigueur le 01 juillet 1983 et est applicable dès que le gouvernement ou l'une de ses institutions réalisent du traitement de renseignements personnels, notamment en matière de sécurité frontalière. Le secteur privé n'est cependant pas soumis à ces dispositions. Tous les principes attachés au traitement de données du RGPD mais également des droits aux personnes sont retrouvables dans cette loi tels que les principes de licéité, de finalité, de conservation limitée des renseignements personnels et le droit d'information.[259]. Cette loi est amenée à évoluer dans un avenir proche. En effet, le 24 novembre 2016, l'ancienne Ministre de la Justice canadienne, Jody-Wilson-Raybould a annoncé au Comité permanent de l'accès à l'information de la protection des renseignements personnels et de l'éthique de la Chambre des communes, avoir déposé un projet de loi n°64 à l'Assemblée nationale du Québec – Loi modernisant des dispositions législatives en matière de protection des renseignements personnels qui ont pour objectif *« de redonner aux citoyens le plein contrôle de leurs renseignements personnels et responsabiliser les organisations qui utilisent nos renseignements »*[260]. Un autre texte à l'échelle fédérale est également à l'étude. En effet, le projet de loi C-11[261] du 17 novembre 2020, toujours en discussion à la Chambre des Communes du Canada, vise principalement à instaurer l'interopérabilité au Canada, doter le Commissariat de réels pouvoirs de sanctions, modifier le régime du consentement afin de le rendre plus systématique et la reconnaissance du droit à l'oubli[262]. Si ce projet est adopté des dispositions de la LPRPDE serait abrogées pour une nouvelle loi plus englobante, la Loi sur la protection de la vie privée des consommateurs (LPVPC).

---

[258] Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5

[259] Rapport d'étape sur les évolutions en matière de législation sur la protection des données au Canada (2001-2007) – Rapport à la Commission européenne, mai 2017

[260] S. DU PERRON, « Projet de loi 64 : une réforme à l'européenne du droit à la protection des renseignements personnels », 17 juin 2020

[261] Bill C-11 of House of Commons of Canada, An Act to enact the consumer privacy protection act and the personal information and data protection tribunal act and to make consequential and related amendments to other acts

[262] W MEE et E. MARSHALL et I. AHMAD, « Projet de loi fédéral sur la réforme de la protection des renseignements personnels dans le secteur privé », 24 novembre 2020

Un tribunal administratif serait créé permettant un recours devant les juges des décisions prises par le Commissaire à la protection de la vie privée. Le principe d'*accountability* serait mis en œuvre. Lors d'une allocution, le 26 mai 2021, le Commissaire à la protection de la vie privée du Canada, Daniel Therrien, s'est montré très favorable à ce texte[263].

131.- Existence d'autorités de régulation – La LPRPDE crée le Commissariat à la protection de la vie privée du Canada[264] qui possède des compétences législatives avec les provinces. Cette autorité de régulation a pour objectif d'accompagner les responsables de traitement, d'informer les personnes sur leurs droits et de veiller au respect des dispositions en la matière. Toute personne concernée peut s'adresser à cette autorité. Le commissaire est un *ombudsman* (un médiateur) indépendant qui peut tout comme la CNIL procéder à des enquêtes, effectuer des recommandations et des rapports au pouvoir législatif. Le Bureau du vérificateur général (ci-après BVG) du Canada effectue des audits des activités exécutives et législatives et peut formuler des recommandations qui ne peuvent avoir un caractère politique[265]. Cette activité est bien plus large que la protection des renseignements personnels car elle concerne toutes les politiques menées. En vertu de l'article 73 de la loi sur la protection des renseignements personnels, le BVG délègue ses missions au coordonnateur de l'accès à l'information et de la protection des renseignements personnels qui fournit une analyse plus spécifique. D'autres autorités existent mais sont davantage spécialisées dans un domaine telles que la sécurité nationale avec le Comité de surveillance des activités de renseignement de sécurité ou encore la Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada.

132.- Particularité au Québec – Deux textes fondamentaux encadrent le droit à la protection des données à caractère personnel au Québec. La loi sur la protection des renseignements personnels adopté en 1994 concerne le secteur privé. Tandis que la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels de 1982 concerne le secteur public. Cette province possède également sa propre autorité de régulation : la Commission d'accès à l'information.

133.- Dans le domaine de la sécurité nationale – Le service canadien du renseignement de sécurité (ci-après SCRS) a pour mission d'enquêter sur les activités qui pourraient menacer la sécurité du Canada et d'établir des rapports au gouvernement. Ces activités sont encadrées par la Loi sur le Service canadien du renseignement de sécurité qui

[263] Allocution prononcée au Symposium sur la protection de la vie privée de l'IAPP de Daniel Therrien, « L'avenir de la réforme des lois sur la protection des renseignements personnels au Canada », 26 mai 2021
[264] https://www.priv.gc.ca/fr
[265] https://www.oag-bvg.gc.ca

comporte également des dispositions relatives à la protection des données à caractère personnel. Le SCRS doit également respecter la Loi sur la protection des renseignements personnels ainsi que la Charte canadienne des droits et libertés. En août 2015, une loi sur la sûreté des déplacements aériens (LSDA) a élargi le mandat du programme de protection des passagers pour permettre au Ministre de la sécurité publique et de la protection civile de mettre en place une liste de personnes dont ils existeraient *« des motifs raisonnables de soupçonner qu'ils participeront ou tenteront de participer à un acte qui menacerait la sureté des transports ou de se déplacer en aéronef dans le but de commettre certaines infractions de terrorisme »*[266]. Cette liste correspond à l'équivalent de la liste de surveillance ETIAS. La LSDA va cependant plus loin car elle autorise le Ministre à conclure des accords pour le transfert de tout ou partie de cette liste à des Etats étrangers.

134.- Un niveau de sécurité jugé adéquat – La politique de protection des renseignements personnels est très proche de celle de l'Union européenne. La Commission européenne a ainsi jugé que le Canada est un Etat où il faut considérer qu'un niveau de protection adéquat des données à caractère personnel existe[267]. Cela signifie donc notamment que les données personnelles collectées dans l'Union européenne peuvent être transférées au Canada, comme c'est le cas depuis 2017 des données des dossiers passagers[268]. Par une lettre adressée en 2017, la direction générale de la justice et des consommateurs de la Commission a souhaité réévaluer la politique du Canada dans ce domaine et a donc réclamé que le gouvernement canadien lui fournisse toutes les informations nécessaires à son évaluation[269]. La rapport rendu en mai 2017 a satisfait la Commission européenne qui a à nouveau jugé le niveau de sécurité suffisant.

135.- Décision politique – La politique de protection des données personnelles dépend de la philosophie de l'Etat (libéralisme ou protectionnisme) qui peut s'expliquer par l'histoire mais également par le contexte politique existant dans l'Etat ou dans la région dans laquelle il s'insère. Cependant, ce choix entre une meilleure sécurité ou une meilleure protection est cornélien. En effet, le Canada et l'Union européenne tente de concilier ces deux notions paradoxales en adoptant des actes législatifs permettant à la fois de meilleurs garanties pour les droits des individus et d'assurer un niveau élevé de sécurité. Cependant, la pratique rend difficile l'existence parallèle de ces textes car la volonté de plus de sécurité finit indubitablement par annihiler les garanties mises en place.

[266] Article 6 de la Loi sur la sûreté des déplacements aériens, L.C.2015, ch.20, 01 août 2015

[267] Décision 2002/2/CE du 20 décembre 2001 constatant le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques

[268] Décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et le Canada 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, 18 octobre 2017

[269] https://www.international.gc.ca/world-monde/international_relations-relations_internationales/eu-ue/

Chapitre II. Le développement d'outils pour une Europe qui protège : la sécurité numérique

Pour être capable de protéger toutes les données collectées et faire face aux nouvelles menaces de plus en plus sophistiquées, l'Union européenne doit avoir une stratégie offensive en matière de cybersécurité (I). Ce développement est la condition fondamentale pour se diriger vers une sécurité organisée autour de l'intelligence artificielle (II).

Section I. Le besoin d'une stratégie offensive de cybersécurité de l'Union européenne

> *« Les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars »*[270]

L'Union européenne a mis en place une règlementation concernant la cybersécurité que tardivement et de manière progressive (I). Elle y établit également des acteurs importants pour veiller au respect de cette règlementation (II).

I. La mise en place progressive d'une réglementation européenne pour faire face aux nouvelles menaces sophistiquées

L'Union européenne a pris conscience que tardivement de la nécessité de se doter d'une règlementation forte en matière de cybersécurité (A). Ce retard l'oblige à accélérer par le biais de nouvelles réformes (B). Pour parvenir à ses ambitions, l'Union soutient financièrement toute ces nouveautés (C).

A. Une prise de conscience tardive

136.- Définitions – Au préalable il est nécessaire de définir deux notions clefs : la cybersécurité et la cyber-résilience. La cybersécurité permet de *« réduire le risque d'atteinte à des infrastructures par des moyens physiques ou mesures de cyberdéfense contre des attaques et des incidents, dans le cadre de l'utilisation de systèmes d'information et de communication »*[271]. La cyber-résilience est « *la capacité à préparer et à s'adapter à des conditions changeantes, de résister et de récupérer rapidement suite*

[270] Jean-Claude JUNCKER, Discours sur l'état de l'Union, 13 septembre 2017
[271] Mémoire Houssama BOUTERBIAT, « Cybersécurité et Cyber-résilience du transport aérien », année universitaire 2019-2020

aux perturbations subies du fait d'attaques ou d'incidents. La résilience est de la gestion de risque »[272]. La cyber-résilience est considérée comme étant un objectif prioritaire de l'Union européenne[273].

137.- Premiers textes législatifs – Bien que les enjeux tournés autour de la cybersécurité soient récents, l'Union européenne n'a compris ces enjeux que récemment. En effet, le premier texte est la Directive 2016/1148[274], dite SRI, qui est entré en vigueur en 2018. Ce texte fondateur en la matière oblige les Etats membres à avoir une stratégie des réseaux et de l'information au niveau national et de désigner une autorité nationale compétente en la matière qui aura pour mission de veiller au respect de l'application de ce texte et de gérer les risques et incidents de sécurité. Cette agence en France est l'Agence Nationale de la Sécurité des Systèmes d'Information (ci-après « ANSSI »). L'Union européenne encourage également la coopération entre les Etats membres avec la création du groupe Computer Security Incident Response Team (ci-après « CSIRT ») qui est composé d'experts et qui a pour unique objectif de réagir en cas d'incident de sécurité. Enfin, tout incident doit désormais être notifié pour permettre une meilleure prise en compte et gestion des risques. Ce texte est à compléter avec la Directive 2013/40[275] qui est plus spécifique sur les attaques contre les systèmes d'information. Elle érige des sanctions et définit des infractions pénales. Les institutions considèrent ces deux textes comme étant le *« noyau dur »* de la règlementation en matière de cybersécurité[276].

B. Une accélération nécessaire en 2020

138.- Réforme SRI2 – Afin de renforcer la résilience des Etats membres, l'Union a soumis, le 16 décembre 2020, une nouvelle proposition de Directive afin de remplacer la Directive SRI[277]. En effet, des inégalités importantes demeurent entre les Etats créant un faible niveau de cyber-résilience et l'absence de réponse commune aux différentes crises ont motivé la décision des institutions européennes. Cette potentielle réforme est également la conséquence du développement grandissant de la cybercriminalité durant la pandémie de la Covid-19 qui a démontré les lacunes de l'application de la Directive

[272] Mémoire Houssama BOUTERBIAT, « Cybersécurité et Cyber-résilience du transport aérien », année universitaire 2019-2020
[273] Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions Stratégie de cybersécurité de l'Union européenne, « Un cyberespace ouvert, sûr et sécurisé », 07 février 2013
[274] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 06 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union
[275] Directive 2013/40/UE du 12 août 2013 relative aux attaques contre les systèmes d'information
[276] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 05 juillet 2016, Renforcer le système européen de cyber résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité
[277] Proposition de directive du Parlement européen et du Conseil du 16 décembre 2020 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union

SRI[278]. Cette proposition de réforme vise donc à renforcer les exigences de sécurité et notamment celles relatives à l'application de la règlementation afin d'obtenir une meilleure harmonisation entre les Etats ce qui implique un renforcement des sanctions pour les Etats qui manquent à leurs obligations. En ce sens, des mesures de surveillance plus strictes sont proposées pour les autorités nationales. Une nouvelle distinction en fonction du degré de risque est également établie : les entités critiques, les entités essentielles et les entités importantes. Une entité critique est *« une infrastructure critique située dans les pays de l'Union européenne et dont l'arrêt ou la destruction aurait un impact considérable sur deux pays de l'Union européenne, au moins »*[279]. L'agence eu-LISA qui gère opérationnellement la sécurité des systèmes d'information européen est considérée comme étant une entité critique. L'apport décisif de ce nouveau texte est la proposition de créer CyCLONe *(Cyber Crisis Liaison Organisation Network)* qui est un réseau européen qui aurait pour mission principale de préparer et gérer de manière coordonnée les futures crises en encourageant les Etats à échanger et partager les informations et connaissances nécessaires à la résolution du risque. Guillaume Poupard, directeur général de l'ANSSI considère que *« CyCLONe est une brique décisive dans la construction d'une Europe de la cybersécurité, résiliente et souveraine »*[280]. Cette proposition est toujours en cours de discussion et aboutira surement à une nouvelle Directive SRI2 dans les prochains mois.

139.- Création d'une unité conjointe de cybersécurité – Dans cette volonté d'accroitre la sécurité des réseaux et des informations, la Commission européenne a annoncé[281], en juin 2021, souhaiter créer une unité conjointe de cybersécurité afin d'avoir une réponse immédiate et efficace en cas d'incidents majeurs. La Commission justifie cette création par l'évolution exponentielle d'incidents graves et dont l'Europe n'est pour l'heure pas toujours capable d'apporter une réaction adéquate et rapide. Cette unité serait une *« plateforme européenne de solidarité et d'assistance pour lutter contre les cyberattaques majeures »*. Margrethe VESTAGER, troisième vice-présidente exécutive de la Commission européenne pour une Europe préparée à l'ère du numérique déclare que *« la cybersécurité constitue une pierre angulaire d'une Europe numérique et connectée. Dans la société actuelle, il est primordial de réagir aux menaces de manière coordonnée. L'unité conjointe de cybersécurité contribuera à la réalisation de cet objectif. Ensemble,*

[278] P. BERTHELET, « Crise du Covid-19 : selon Europol, le cybervirus se répand de manière exponentielle », 15 avril 2020

[279] Communication de la Commission du 12 décembre 2006 sur un programme européen de protection des infrastructures critiques

[280] Loic DUVAL, News informatique, *CyCLONe : Comment l'Europe se prépare aux crises cyber à venir*, le 29 septembre 2020

[281] Communiqué de presse de la Commission européenne du 23 juin 2021, « Cybersécurité de l'Union européenne : la Commission propose la création d'une unité conjointe de cybersécurité afin d'intensifier la réaction aux incidents majeurs de sécurité »

nous pouvons faire une réelle différence »[282]. Cette unité sera créée au sein de l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) avec quatre étapes de construction[283]. Dès le 31 décembre 2021, une évaluation et une identification des capacités opérationnelles de l'Union et des risques éventuels sera menée. Le 30 juin 2022, sur la base de cette évaluation, un rapport sera remis aux institutions de l'Union afin de définir les rôles et les responsabilités des participants à cette unité. Le 31 décembre 2022, l'unité devrait être opérationnelle et permettra dès juin 2023 d'impliquer les acteurs du secteur privé.

140.- Nouvelle stratégie pour la décennie numérique – Lors d'une communication conjointe, le Parlement européen et le Conseil ont annoncé leur stratégie de cybersécurité pour la prochaine *« décennie numérique »*[284]. A cette occasion, alors que la coopération entre les Etats membres en matière de cybersécurité est encore défaillante, ces deux institutions souhaitent que l'Union collabore davantage avec les pays tiers et les organisations internationales dans ce domaine. Consciente du retard qui a été pris notamment sur la Chine et les Etats-Unis, l'Union européenne se donne pour objectif de renforcer sa position à l'échelle mondiale et obtenir une réelle souveraineté en la matière sans dépendance des pays tiers. Cela s'explique notamment par les tensions géopolitiques grandissantes et l'exploitation du cyberespace à des fins idéologiques et politiques. L'Union européenne se fixe des objectifs ambitieux qu'il sera primordial de tenir car la multiplication de systèmes d'information et le nombre considérable de données à caractère personnel traitées, une sécurité irréprochable devra être assurée afin de maintenir une confiance, déjà fragile, avec la population.

3. Le soutien financier de l'Union européenne

141.- Programme Digital Europe – Tous ces objectifs doivent être tenus mais surtout soutenus financièrement. Ainsi, l'Union a mis en place le Programme Digital Europe, un programme de financement qui vise à apporter un soutien dans le développement *« des supercalculateurs, de l'intelligence artificielle, de la cybersécurité et des compétences numériques avancées »*[285]. Pour ce faire, un budget de 7,5 milliards d'euros a été fixé[286]. La partie sur la cybersécurité sera géré par le futur centre européen de compétences

[282] Le Monde du Droit, « Cybersécurité de l'UE : la Commission propose une Unité conjointe de sécurité afin de renforcer la réaction face aux incidents de sécurité majeurs », 23 juin 2021
[283] Infographie de la Commisson européenne du 23 juin 2021, Joint Cyber Unit
[284] Communication conjointe au Parlement européen et au Conseil du 16 décembre 2020, « La stratégie de cybersécurité de l'UE pour la décennie numérique »

[285] https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[286] Règlement (UE) n° 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique

industrielles, technologiques et de recherche en matière de cybersécurité, qui sera basé à Bucarest.

II. L'établissement et le développement d'acteurs impliqués dans la cybersécurité

L'Agence européenne chargée de la sécurité des réseaux et de l'information (A) et l'Agence nationale de la sécurité des systèmes d'information (B) sont les acteurs majeurs impliqués dans la cybersécurité mais avec un degré différent en raison de l'importance qu'accordent les Etats membres à leur souveraineté.

A. A l'échelle européenne : Agence européenne chargée de la sécurité des réseaux et de l'information

142.- Le fonctionnement et les missions de l'ENISA – L'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a été instituée le 10 mars 2004 pour *« assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de l'Union et à favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information »*[287]. Cette agence a connu plusieurs réformes en 2013[288] et 2019, avec le Cybersecurity Act[289], dont la dernière avait pour but de remédier aux ressources insuffisantes, au mandat limité qui l'empêchait d'avoir une vision à long terme mais surtout de dépasser les désirs et intérêts des Etats membres. Un réseau des agents de liaison nationaux a été créé pour faciliter la coopération et l'échange d'informations entre l'ENISA et les Etats membres[290]. L'ENISA ne doit pas être considérée comme une agence supranationale mais comme une *« plateforme de facilitation »*[291]. En effet, l'ENISA n'est pas une autorité de contrôle ou de sanction car pour ne pas empiéter sur la souveraineté des Etats, ses missions sont bornées à du conseil et de l'assistance[292]. La proposition de Directive SRI2 donne de nouvelles missions à l'agence qui devrait tenir un registre européen des vulnérabilités et assurer le secrétariat du réseau CyCLONe[293].

---

[287] Règlement (CE) n° 460/2004 du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information

[288] Règlement (UE) n° 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence de l'Union européenne pour la sécurité des réseaux et de l'information (ENISA)

[289] Règlement (UE) n° 2019/881 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications

[290] https://www.enisa.europa.eu/

[291] E. BOTHOREL, Rapport d'information pour la Commission des affaires européennes de l'Assemblée nationale sur les effets de la transformation de l'agence européenne ENISA sur l'architecture de la cybersécurité européenne et les conséquences plus larges de l'adoption du paquet cybersécurité, 25 juillet 2019

[292] J. EYNARD, « Agence européenne chargée de la sécurité des réseaux et de l'information », *Répertoire IP/IT et Communication / Cybersécurité,* janvier 2021

[293] Article 6 et article 14 de la Proposition de directive du Parlement européen et du Conseil du 16 décembre 2020 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union

B. A l'échelle nationale : Agence nationale de la sécurité des systèmes d'information

143.- Le fonctionnement et les missions de l'ANSSI – L'agence nationale de la sécurité des systèmes d'information (ANSSI) ayant été créée par décret le 07 juillet 2009[294] a remplacé la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI). Cette autorité nationale est compétente en matière de sécurité des réseaux et des systèmes d'information en vertu de l'article 8 de la Directive SRI et est l'unique interlocuteur pour la coopération transfrontalière entre les Etats membres et leur autorité nationale. Pour ce faire, elle accompagne, soutient et forme, également les administrations publiques notamment afin qu'elles parviennent à un haut niveau de cybersécurité. Elle participe également à la recherche pour le développement de nouvelles technologies[295]. Doté d'un centre de cyberdéfense, elle veille de manière continue aux cybermenaces que la France pourrait rencontrer, réagit et alerte en cas de cyberattaque. Depuis le *Cybersecurity Act*[296] adopté en 2019, l'ANSSI est également une autorité de certification en matière de cybersécurité. Ainsi, elle peut réaliser des audits et entrer dans les locaux des organismes qui possèdent un certificat européen de cybersécurité et procéder à une enquête. Si cette dernière est insatisfaisante et révèle des violations importantes, des sanctions peuvent être infligées pouvant aller jusqu'au retrait du certificat[297]. L'ENISA effectue uniquement une évaluation de l'ANSSI tous les cinq ans et n'a qu'un rôle de coordination envers l'ANSSI qui elle est une véritable autorité de contrôle et de sanction. En outre, l'autorité qui supervise l'ANSSI n'est pas une agence européenne mais l'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) qui est une administration gouvernementale. Cela démontre l'attachement qu'ont les Etats membres sur leur souveraineté en matière de cybersécurité. Houssama BOUTERBIAT, ancien étudiant de l'IFURTA, qualifie cette agence de *« Cerbère de la cybersécurité française »*[298].

Section II. Vers une sécurité organisée autour de l'intelligence artificielle

La sécurité de demain est incontestablement tournée vers l'intelligence artificielle (ci-après IA) où l'Union décide actuellement d'élaborer un cadre juridique autour de ces enjeux (I). Cette notion est déjà en application dans la vie des voyageurs Européens et est amenée à se développer dans les prochaines années (II).

[294] Décret n°2009-834 du 07 juillet 2009, JO 8 juillet n°156
[295] https://www.ssi.gouv.fr/
[296] Article 58 du Règlement (UE) n° 2019/881 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications
[297] J. EYNARD, « Agence européenne chargée de la sécurité des réseaux et de l'information », *Répertoire IP/IT et Communication / Cybersécurité,* janvier 2021
[298] Mémoire Houssama BOUTERBIAT, « Cybersécurité et Cyber-résilience du transport aérien », année universitaire 2019-2020

« En matière d'intelligence artificielle, la confiance n'est pas un luxe mais une nécessité absolue. En adoptant ces règles qui feront date, l'Union prend l'initiative d'élaborer de nouvelles normes mondiales qui garantiront que l'IA soit digne de confiance. En établissant les normes, nous pouvons ouvrir la voie à une technologue éthique dans le monde entier tout en préservant la compétitivité de l'Union. A l'épreuve du temps et propices à l'innovation, nos règles s'appliqueront lorsque c'est strictement nécessaire : quand la sécurité et les droits fondamentaux des citoyens de l'Union sont en jeu »[299].

I. L'élaboration d'un cadre juridique européen sur l'intelligence artificielle

144.- Définition – L'intelligence artificielle a été mis en lumière grâce au livre *Computing Machinery and Intelligence* du mathématicien Alain Turing en 1950. Cette notion peut être définie comme étant *« l'ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence humaine »*[300].

145.- Rapport de FRONTEX – En mars 2021, FRONTEX a rendu aux institutions européennes un rapport concernant les avantages et les possibilités que pouvait apporter l'intelligence artificielle dans la gestion des frontières[301]. L'agence européenne met en avant que l'IA permettrait de faciliter la prise de décision, d'être plus efficace dans les interventions, de mieux gérer les données afin de diminuer la marge d'erreur quant à l'identification et l'authentification. Cependant l'IA demande une quantité considérable de données pour pouvoir obtenir des résultats, ce qui exige d'accroitre la collecte de données tout en respectant les droits fondamentaux comprenant également le droit à la protection des données à caractère personnel. En outre, les applications d'IA sont aujourd'hui encore très chères même si on assiste à une démocratisation.

146.- Artificial Intelligence Act – L'IA est un enjeu dont les institutions européennes se sont saisies dès 2018 mais davantage sur un terrain de réflexion et non de mise en place d'une règlementation. Il était nécessaire de définir la vision de l'Union sur les opportunités mais également les risques qu'induisent l'IA. Ce travail de réflexion se retrouve dans la première communication de la Commission en avril 2018[302]. Après le

[299] https://ec.europa.eu/france/news/20210421/nouvelles_regles_europeennes_intelligence_artificielle_fr
[300] Définition Larousse 1996
[301] FRONTEX, Report Artificial Intelligence – Based capabilities for the European Border and Coast Guard, 21 mars 2021
[302] Communication de la Commission au Parlement européen, au Conseil européen, au Comité économique et social européen et au Comité des régions du 25 avril 2018, « L'intelligence artificielle pour l'Europe »

livre blanc sur l'intelligence artificielle[303], la Commission européenne a annoncé le 21 avril dernier un projet de Règlement ayant pour objectif de mettre en place le premier cadre juridique européen sur l'IA : *Artificial Intelligence Act*[304]. L'apport principal de ce nouveau texte est l'établissement de différents niveaux de risques où chaque niveau correspond à des règles de plus en plus strictes[305]. Le premier stade est le *« risque minime »* où aucune intervention n'est nécessaire puisqu'il n'existe aucun risque en termes de sécurité et vis-à-vis des droits fondamentaux. Le *« risque limité »* impose une obligation de transparence auprès de l'utilisateur. Le *« risque élevé »* fait référence aux systèmes liés à la gestion de la migration et le contrôle aux frontières ou encore tout ce qui concerne l'administration de la justice. Les conditions suivantes devront être mises en place obligatoirement :

> *« - Systèmes adéquats d'évaluation et d'atténuation des risques ;*
> *- Qualité élevée des ensembles de données alimentant le système afin de réduire au minimum les risques et les résultats ayant un effet discriminatoire*
> *- Enregistrement des activités afin de garantir la traçabilité des résultats*
> *- Documentation détaillé fournissant toutes les informations nécessaires sur le système et sur sa finalité pour permettre aux autorités d'évaluer sa conformité*
> *- Informations claires et adéquates à l'intention de l'utilisateur, contrôle humain approprié pour réduire au minimum les risques, niveau élevé de robustesse, de sécurité et d'exactitude »*

Enfin, le « risque inacceptable » correspond à une menace manifeste pour la sécurité. Toutes applications seront donc interdites. Cela fait référence aux applications qui manipulent le comportement humain par exemple. Cette proposition de Règlement est à mettre en perspective avec le plan coordonné entre les Etats membres et l'Union européenne[306] qui expose les conditions nécessaires pour le bon développement de l'IA. On remarque que la confiance est une modalité *sine qua none* à la réussite de l'épanouissent de l'IA en Europe, qui constitue une réelle préoccupation de la Commission européenne. En effet, les populations doivent y adhérer et cela ne peut se réaliser sans pédagogie sans relation de confiance dans ces systèmes. Cette question est l'un des défis de l'Union. Et pour cause, à l'heure de l'inquiétude des Européens sur la collecte et le traitement incessant de leurs données personnelles et le respect de leur vie privée, seront-ils prêts à consentir à ces nouveaux systèmes supplémentaires alors que

[303] Livre blanc de la Commission européenne – Intelligence artificielle, « Une approche européenne axée sur l'excellence et la confiance », 19 février 2020
[304] Proposition de Règlement du Parlement européen et du Conseil du 21 avril 2021 établissant des règles harmonisées en matière d'intelligence artificielle
[305] https://ec.europa.eu/france/news/20210421/nouvelles_regles_europeennes_intelligence_artificielle_fr
[306] https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

leur consentement ne leur sera pas demandé, en ce qui concerne le contrôle des frontières ?

II. L'application de l'intelligence artificielle dans la gestion de la migration et le contrôle aux frontières

L'intelligence artificielle est dès à présent utilisée dans la gestion de la migration et le contrôle aux frontières grâce à l'utilisation de la reconnaissance faciale (A) qui est amenée à se développer puisqu'un détecteur de mensonge est actuellement à l'étude (B).

A. L'utilisation de la reconnaissance faciale dans la gestion des frontières françaises

147.- Définition – La reconnaissance faciale est définie par la CNIL comme étant une *« technique qui permet à partir des traits de visage d'authentifier une personne, c'est-à-dire vérifier qu'une personne est bien celle qu'elle prétend être, ou d'identifier une personne, c'est-à-dire de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données »*[307].

148.- Passage Automatisé Rapide aux Frontières Extérieures – Le système Passage Automatisé Rapide aux Frontières Extérieures (ci-après « PARAFE ») existe depuis 2009 à l'aéroport de Paris Charles-de-Gaulle. Depuis, il s'est développé pour être présent aujourd'hui dans 7 aéroports métropolitains, la gare du Nord, la gare de Saint Pancras et les sites de Coquelles et Cheriton de part et d'autre de l'Eurotunnel. En 2019, plus de 11 millions de voyageurs ont utilisé les sas du PARAFE et il a été considéré que 45% des passagers sont éligibles à ce système, ce qui montre son importance[308]. Le PARAFE est un système de contrôle automatisé des frontières françaises qui se base sur une authentification des données biométriques et sur la reconnaissance faciale. Pour rappel, les données biométriques sont également des données à caractère personnel qui sont reconnues par la Cour Européenne des Droits de l'Homme (ci-après « CEDH »)[309]. La CNIL a cependant autorisé le traitement de ces données et les critères du visage de la personne pour vérifier son identité[310]. Le PARAFE utilise l'interopérabilité de systèmes d'information comme le VIS, SLTD, le fichier des personnes recherchées, et l'IA à travers la reconnaissance faciale. Les personnes éligibles à passer par les sas du PARAFE sont uniquement les personnes majeures titulaires d'un passeport biométrique de l'un des

[307] https://www.cnil.fr/fr/definition/reconnaissance-faciale
[308]https://www.immigration.interieur.gouv.fr/Europe-et-International/La-circulation-transfrontiere/Le-passage-rapide-aux-frontieres-exterieures-PARAFE
[309] CEDH, S. et Marper c. Royaume-Uni, 04 décembre 2008, requêtes n°30562/04 et 30566/04
[310] CNIL, avis du 28 janvier 2016 délibération n°2016-012

pays membre de l'Union ou de la Suisse, l'Islande, la Norvège ou le Liechtenstein[311]. La CNIL a autorisé[312] en 2019, l'extension de l'utilisation des PARAFE pour les mineurs d'au moins 12 ans et les ressortissants de pays tiers qui possèdent une carte de séjour de membre de la famille d'un citoyen de l'Union. Ce système conserve les données personnelles pendant cinq années sauf pour les mineurs où la durée limite est fixée à trois années L'un des arguments brandis pour la mise en place du système PARAFE est l'amélioration de l'expérience du passager. Il est vrai que cela permet de fluidifier le nombre de voyageurs avec une réduction du temps au poste frontière à 10 à 15 secondes[313].

149.- Controverse – Les journaliste Jean-Pierre Cannet et Arthur Bouvert ont démontré dans leur reportage[314] des failles de sécurité importantes dans le système PARAFE. En effet, les deux ont réussis à passer les sas du PARAFE en échangeant les passeports grâce à une fausse peau sur laquelle l'empreinte digitale de leur partenaire était imprimé. À la vue de la controverse suscitée, le système PARAFE a été remplacé pour se baser désormais sur la reconnaissance faciale du voyageur et plus ses données biométriques. Cette modification restreint fortement les possibilités de fraude.

150.- Une solution aux passagers non-admissibles ? – L'autre argument en faveur de ce système est la lutte contre les fraudes documentaires. Le système PARAFE concerne aujourd'hui les citoyens européens mais il pourrait être une solution imparable aux passagers non-admissibles sur le territoire français. En effet, ce système pourrait être étendu aux ressortissants de pays tiers. Ainsi, l'Etat exercerait pleinement ses missions régaliennes et mettrait fin à la lourde responsabilité supportée par les compagnies aériennes aujourd'hui dans la vérification documentaire. Cette extension nécessiterait effectivement d'amplifier l'interopérabilité avec les systèmes d'information européens déjà mis en place. Ce déploiement obligerait également les autorités publiques à investir considérablement dans ce système mais leur permettrait à long terme d'être plus efficace dans le contrôle des documents de voyage et donc dans la surveillance des frontières qui pose tant de problèmes.

151.- La reconnaissance faciale utilisée par les compagnies aériennes – Cette technologie est désormais utilisée, en phase d'expérimentation, par certaines compagnies aériennes. Le système MONA, développé par l'entreprise Idemia[315], est actuellement disponible aux aéroports de Paris-Orly et Lyon-Saint-Exupéry. A Paris, cette technologie

[311] Mémoire Abdullah SEN, « Reconnaissance Faciale », année universitaire 2018-2019
[312] CNIL, avis du 29 mars 2019 délibération n°2019-027
[313] Mémoire Abdullah SEN, « Reconnaissance Faciale », année universitaire 2018-2019
[314] Reportage Cash Investigation, France 2, « Le business de la peur », 22 septembre 2015
[315] https://www.idemia.com/fr

est disponible pour tous les vols à destination du Maroc opérés par la compagnie Transavia France. A Lyon, elle concerne tous les vols pour Lisbonne opérés par Transavia France et la TAP Air Portugal[316]. Air Caraïbes devrait également tester MONA pour ses vols vers les DOM-TOM. La reconnaissance faciale permet à ces passagers de ne plus présenter leur carte d'embarquement ni leur pièce d'identité, puisque leur visage leur permet d'enregistrer leurs bagages et passer les points de contrôle plus rapidement[317]. MONA peut être utilisé par tous les passagers majeurs, quelle que soit leur nationalité, contrairement au système PARAFE[318]. En outre, basé sur le volontariat, MONA permet de requérir un réel consentement du passager. Pour profiter de ce nouveau système, le passager doit se présenter à une borne biométrique, présente au comptoir d'enregistrement, afin de scanner sa pièce d'identité ainsi que sa carte d'embarquement et d'enregistrer son visage. La borne relie ensuite toutes ces informations afin de reconnaître le passager aux différents points de contrôle. La société Aéroports de Paris (ci-après « ADP ») estime que ce système permet un gain de temps de 30 min par rapport à un enregistrement classique. Les conséquences quant au traitement de données à caractère personnel est limité puisque les données sont *« supprimées dès le décollage de l'avion »*[319]. Des inconvénients sont cependant à souligner afin d'améliorer ce système et pouvoir exploiter toutes ses possibilités. En effet, les ressortissants soumis à l'obligation d'un visa, et bientôt de l'ETIAS, effectuent-t-ils deux contrôles ou bien MONA enregistre-t-il ces documents de voyages supplémentaires ? Comment concilier le système PARAFE et MONA sachant que les critères d'éligibilité à ces dispositifs ne sont pas les mêmes ? La plus grande difficulté à surmonter est que MONA est mis en place uniquement sur le territoire français et non sur les escales extérieures des compagnies aériennes. Si l'objectif est, en plus de fluidifier le parcours voyageur, de gérer plus efficacement la vérification documentaire des potentiels passagers non-admissibles, MONA devra s'exporter en dehors de l'espace Schengen. Cependant, le manque de cadre légal dans ces Etats peut rendre cette ambition impossible.

B. Le détecteur de mensonge aux portes des frontières françaises : iBorderCtrl

152.- Développement du iBorderCtrl – iBorderCtrl *(Contrôle intelligent des frontières)* est un système développé par la Manchester Metropolitan University qui est un détecteur de mensonge par reconnaissance faciale. iBorderCtrl réalise un entretien virtuel avec le passager au poste frontière en demandant par exemple le motif du séjour. Capable

[316] https://www.lyonmag.com/article/110634/lyon-mona-le-nouveau-systeme-de-reconnaissance-faciale-a-l-aeroport-saint-exupery
[317] https://www.youtube.com/watch?v=bcokMzyt8sk
[318] https://www.parisaeroport.fr/passagers/preparation-vol/votre-voyage/la-reconnaissance-du-visage
[319]https://www.usine-digitale.fr/article/l-aeroport-d-orly-teste-la-reconnaissance-faciale-a-l-embarquement-avec-la-compagnie-transavia.N1074209

d'identifier 38 expressions faciales, iBorderCtrl analyse le comportement du passager et détermine s'il ment ou non. Il dirige ensuite le voyageur soit dans des files d'attentes rapides ou vers un garde-frontière qui effectuera un contrôle plus approfondi[320]. Financée depuis par la Commission européenne, ce système futuriste est désormais en phase de test en Grèce, Hongrie et Lettonie. Avec un taux de réussite de l'ordre de 75%, l'objectif est qu'il investisse les aéroports européens d'ici 2023. Dans une vidéo promotionnelle, Keeley Crockett, professeur à l'Université de Manchester, souhaite rassurer en expliquant que iBorderCtrl *« ne prendra pas de décision automatisée, mais produit une évaluation du risque »*[321]. Ce développement de système qui irait jusqu'à analyser les émotions, la psychologie d'un voyageur au nom de la sécurité n'est-il pas excessif ? Quant est-il de la protection des données à caractère personnel ? Ces données relèvent de plus en plus de l'intime de la personne. Le corps devient par contrainte la carte d'identité de demain.

[320] https://www.ouest-france.fr/europe/ue/un-systeme-d-intelligence-artificielle-pour-garder-les-frontieres-de-l-ue
[321] https://www.youtube.com/watch?v=9fsd3Ubqi38

CONCLUSION

> « Un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'un, ni l'autre, et finit par perdre les deux ».
>
> Benjamin Franklin

La remise en cause du système, instauré par les Accords de Schengen, est principalement due aux problématiques des contrôles des frontières extérieures qui sont exacerbées par l'instauration d'une méfiance entre les différents Etats membres et la montée de l'euroscepticisme. Pourtant, l'Union européenne, qui apparaît comme le coupable idéal, a consenti à des efforts importants qui sont aujourd'hui jugés insuffisants face à la crise existentielle que traverse l'espace Schengen. Une application plus rigoureuse des principes de Schengen et le retour d'une véritable confiance mutuelle sont les clefs du sauvetage de cette formidable construction. La « Stratégie Schengen » de 2021 sera-t-elle suffisante ? Sera-t-elle à la hauteur des défis et des obstacles qui se présenteront à l'avenir ?

L'instauration de l'ETIAS, en mai 2022, se révèle être une nécessité pour mieux appréhender les risques que pourraient constituer les migrants vis-à-vis de l'ordre public et la santé publique mais également pour que les Etats soient mieux informés sur les déplacements des individus. Cette autorisation de voyage provoque des mutations profondes. En effet, l'ETIAS permet aux agences européennes FRONTEX et eu-LISA de renforcer leurs positions dans le contrôle des frontières et leur place dans la coopération entre les Etats. C'est également le synonyme de la mise en place de l'interopérabilité qui a pour but d'assurer une surveillance plus efficace et dont les institutions européennes lui accordent une forte attente. Enfin, l'ETIAS pourrait être la preuve du retour de l'Etat dans ses missions régaliennes de vérification documentaire, permettant ainsi d'alléger la lourde responsabilité des transporteurs aériens quant au régime des passagers non-admissibles sur le territoire français.

L'interopérabilité est le résultat d'une expansion poussée du développement des systèmes d'information européens ce qui a des conséquences non négligeables sur les données personnelles. En effet, elle a un effet multiplicateur quant à la collecte et aux traitements des données à caractère personnel.

Cependant, cette solution doit être mise en parallèle avec le développement du droit à la protection des données à caractère personnel depuis les années 1970 et dont la

consécration s'est faite en 2016 avec l'avènement du RGPD. En effet, ce fameux texte assure un niveau de sécurité élevé des données personnelles et des droits hautement protecteurs qui sont garantis par des autorités judiciaires et de régulation.

Bien que le Règlement instituant l'ETIAS promet une protection élevée des données personnelles des demandeurs, elle constitue néanmoins une réelle ingérence au nom de la sécurité publique. Cette notion s'avère être vague et discutable quant à la marge d'appréciation et à la liberté laissée aux gouvernants. Ainsi, il serait sans doute exagéré de parler d'une remise en cause du RGPD mais il existe bien une réelle atteinte aux principes qui découlent de ce texte.

Les exemples étrangers démontrent que le choix entre sécurité et protection, est politique et économique. Cet équilibre cornélien à trouver démontre la vision qu'ont les gouvernants sur la société.

Par l'étude des futurs projets, il peut être constaté que les dirigeants européens ont clairement décidé d'opter pour plus de sécurité, avec un accroissement notable des collectes et traitements des données à caractère personnel. La sécurité de demain nécessitera donc un niveau de cybersécurité renforcé et le développement d'une meilleure cyber-résilience face à des menaces de plus en plus sophistiquées. L'Union européenne qui était en retard dans ce domaine par rapport à d'autres grandes puissances mondiales a décidé d'accélérer de manière significative son action en menant une stratégie offensive dès 2021.

Ce prérequis est fondamental car la sécurité de demain sera indubitablement une sécurité numérique avec le développement exponentiel de l'intelligence artificielle. En effet, l'Union européenne est sur le point de mettre en place un cadre juridique pour permettre son utilisation et notamment dans la gestion des migrants et des contrôles aux frontières. Quel sera l'avenir des pièces d'identité et des visas ? Le corps des individus remplacera-t-il ces documents dans un futur proche ? C'est en tout cas le chemin qui est en train d'être pris.

BIBLIOGRAPHIE

I. Traités

- Conventions

Convention portant règlement n°ation de la navigation aérienne, 13 octobre 1919

Annexe 9 de la Convention relative à l'aviation civile internationale, « Facilitation », 07 décembre 1944

Charte des Nations unies du 26 juin 1945

Convention européenne des droits de l'Homme du 04 novembre 1950

Accord européen sur le régime de circulation des personnes entre les pays membres du Conseil de l'Europe, 13 décembre 1957

Traité instituant l'Union économique Benelux du 03 février 1958

Convention des Nations Unies sur la mer territoriale et la zone contiguë, 29 avril 1958

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

Convention de Vienne sur le droit des traités, 23 mai 1969

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, n°108, Conseil de l'Europe, 28 janvier 1981

Convention des Nations Unies sur le droit de la mer, 10 décembre 1982

Accord entre la France et la République fédérale d'Allemagne du 13 juillet 1984 relatif à la suppression graduelle des contrôles à la frontière franco-allemande

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

Convention d'application de l'accord de Schengen du 14 juin 1985 du 19 juin 1990 entre les gouvernements des Etats de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes

Convention de 1990 relative à la détermination de l'Etat responsable de l'examen d'une demande d'asile présentée dans l'un des Etats membres des Communautés européennes

Charte des droits fondamentaux de l'Union européenne, du 18 décembre 2000

- Règlements

Règlement (CE) n°2725/2000 du Conseil du 11 décembre 2000 concernant la création du système Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin

Règlement (CE) n°539/2001 du Conseil du 15 mars 2001 fixant la liste des pays tiers dont les ressortissants sont soumis à l'obligation de visa pour franchir les frontières extérieures des Etats membres et la liste de ceux dont les ressortissants sont exemptés de cette obligation

Règlement (CE) n°407/2002 du Conseil du 28 février 2002 fixant certaines modalités d'application du règlement (CE) n°2725/2000 concernant la création du système Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin

Règlement (CE) n°460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information

Règlement (CE) n°1030/2002 du Conseil du 13 juin 2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers

Règlement (CE) n°2007/2004 du Conseil du 26 octobre 2004 portant création d'une Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des Etats membres de l'Union européenne

Règlement (CE) n°562/2006 du Parlement européen et du Conseil 15 mars 2006 établissant un code communautaire relatif au régime de franchissement des frontières par les personnes

Règlement (CE) n°1986/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'accès des services des Etats membres chargés de l'immatriculation des véhicules au Système d'Information Schengen de deuxième génération

Règlement (CE) n°1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du Système d'Information Schengen de deuxième génération

Règlement (CE) n°767/2008 du Parlement européen et du Conseil du 09 juillet 2008 concernant le système d'information sur les visas et l'échange de données entre les Etats membres sur les visas de court séjour

Règlement (CE) n°859/2008 de la Commission du 20 août 2008 en ce qui concerne les règles techniques et procédures administratives communes applicables au transport commercial par avion

Règlement (CE) n°810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code des visas pour l'Union européenne

Règlement (UE) n°1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

Règlement (UE) n°526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée des réseaux et de l'information (ENISA)

Règlement (UE) n°1053/2013 du Conseil du 07 octobre 2013 portant création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen

Règlement (UE) n°2016/399 du Parlement européen et du Conseil du 09 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes

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

Règlement (UE) n°2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes

Règlement (UE) n°2017/458 du Parlement européen et du Conseil du 15 mars 2017 modifiant le Règlement (UE) 2016/299 en ce qui concerne le renforcement des vérifications dans les bases de données pertinentes aux frontières extérieures

Proposition de Règlement du Parlement européen et du Conseil du 29 juin 2017 relatif à l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

Règlement (UE) n°2017/2225 du Parlement européen et du Conseil du 30 novembre 2017 en ce qui concerne l'utilisation du système entrée/sortie

Règlement (UE) n°2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système entrée/sortie pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des Etats membres et portant détermination des conditions d'accès à l'EES à des fins répressives

Règlement (UE) n°2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

Règlement (UE) n°2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA)

Règlement (UE) n°2019/881 du Parlement européen et du Conseil relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications

Règlement (UE) n°2019/816 du Parlement européen et du Conseil 17 avril 2019 portant création d'un système centralisé permettant d'identifier les Etats membres les informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN)

Règlement (UE) n°2019/817 du Parlement européen et du Conseil du 17 avril 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union Européenne dans le domaine des frontières et des visas

Règlement (UE) n°2019/818 du Parlement européen et du Conseil du 18 avril 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union Européenne dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration
Règlement (UE) n°2019/1155 du Parlement européen et du Conseil du 20 juin 2019 portant modification du règlement (CE) n°810/2009 établissant un code communautaire des visas
Proposition de Règlement du Parlement européen et du Conseil du 21 avril 2021 établissant des règles harmonisées en matière d'intelligence artificielle
Règlement (UE) n°2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique

- Directives

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/CE du Parlement et du Conseil 29 avril 2009 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des Etats membres
Directive 2013/40/UE du Parlement européen et du Conseil 12 août 2013 relative aux attaques contre les systèmes d'information
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 poursuite en la matière ou l'exécution de sanction pénales, et à la libre circulation de ces données
Directive (UE) 2016/1148 du Parlement européen et du Conseil du 06 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union
Proposition de Directive du Parlement européen et du Conseil du 16 décembre 2020 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union

- Décisions

Décision 2002/2/CE du 20 décembre 2001 constatant le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques

Décision 2004/512/CE du Conseil du 08 juin 2004 portant création du système d'information sur les visas (VIS)
Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du Système d'Information Schengen de deuxième génération
Décision cadre 2009/316/JAI du 06 avril 2009 relative à la création du système européen d'information sur les casiers judiciaires (ECRIS)
Décision cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les Etats membres (ECRIS)
Décision d'exécution (UE) 2016/2296 de la Commission européenne du 16 décembre 2016 constatant le niveau de protection adéquat des données à caractère personnel assuré par certains pays
Décision du Conseil du 18 octobre 2017 autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et le Canada 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
Décision n°2019/969 et Décision n°2019/970 de la Commission européenne du 22 février 2019
Décision n°2020/971 de la Commission du 26 février 2019

- Résolution

Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures

- Lois françaises

Loi n°78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
Loi n°92-190 du 26 février 1992 relative aux conditions d'entrée et de séjour des étrangers en France
Loi n°2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité
Loi n°2004-801 du 06 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme
Loi n°2016-274 du 07 mars 2016 relative au droit des étrangers en France

Loi n°2016-1321 du 07 octobre 2016 pour une République numérique
Loi n°2018-494 du 20 juin 2018 relative à la protection des données personnelles

- Ordonnance et décret

Ordonnance n°45-2658 du 02 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France
Décret n°2009-834 du 07 juillet 2009, JO 8 juillet n°156

- Codes

Code de l'entrée et du séjour des étrangers et du droit d'asile
Code des transports
Code pénal

- Lois étrangères

Privacy Act de 1974
Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5
Bill C-11 of House of Commons of Canada, An Act to enact the consumer privacy protection act and the personal information and data protection tribunal act and to make consequential and related amendments to other acts
Loi sur la sûreté des déplacements aériens, L.C.2015, ch.20, 01 août 2015

II. <u>Manuels et cours universitaires</u>

F. MATTATIA, « RGPD et droit des données personnelles », 4e édition, paru en septembre 2019
S. WARREN and L. BRANDEIS, "The Right to Privacy", 1890
Cours de Droit aérien, Madame LABORDE DIT BOURIAT, année universitaire 2020-2021
Cours de Droit international des espaces et de l'environnement de Madame POIRAT Florence, année universitaire 2019-2020
Cours de Droit européen des personnes, Mme SAULNIER-CASSIA Emmanuelle, année universitaire 2019-2010

III. Thèses et mémoires

Mémoire de Catherine MSELLATI, « La Convention d'application de l'accord de Schengen et ses implications en matière de transport aérien », Octobre 1996
Mémoire de Julie DURAFFOURD, « Le transport par air de passagers non admissibles », années universitaire 2018-2019
Mémoire Houssama BOUTERBIAT, « Cybersécurité et Cyber-résilience du transport aérien », année universitaire 2019-2020
Mémoire Abdullah SEN, « Reconnaissance Faciale », année universitaire 2018-2019

IV. Répertoires et encyclopédies

Dictionnaire Larousse, 1996
Dico du commerce international
Vocabulaire juridique, Gérard Cornu, 13e édition, Association Henri Captant

V. Articles

P. WEIL, Le Nouvel Observateur, 7-13 août 1997
H. Labayle « Schengen, un espace dans l'impasse », *Revue Europe,* Mars 2016
H. Labayle, « Schengen, un coupable idéal », *GDR*, 25 novembre 2015
Y. PASCOUAU, Question d'Europe n°392 du 17 mai 2016, Fondation Robert Schuman
C. DIRE, « Le concept de gestion intégrée des frontières », *Revue de l'Union européenne*, p.475
G. Georgi « Rutte pours cold water on Bulgaria's Schengen and Eurozone dreams", *Euractiv*, 07/02/2018
A. KARGL, « FRONTEX, symbole d'une gestion des frontières européennes en évolution », publié par l'ANAJ-IHEDN, 1 mars 2018
G.Serra et R. Angrisani, « Espace Schengen et Systèmes d'information : le rôle de l'agence Eu-LISA », Février 2016
C. BLUMANN, « La Frontière », 1980
J-M. SOREL, « Frontière internationale », *Répertoire de droit international*, Juillet 2017
F. GAZIN, « Frontières externes à l'Union européenne : principe des contrôles généralisés », *Répertoire de droit européen*, Janvier 2020
E. Brouwer, "Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information System", Leiden, *Martius Nijhoff Publishers*, 2008
J. MOLINIER, « Les Agences de l'Union européenne », *Revue du droit européen*, 2011

P. BERTHELET, « L'Agence de sécurité des réseaux est une agence « performante » et « de plus en plus importante », 06 septembre 2017
P. BERTHELET, « Crise du Covid-19 : selon Europol, le cybervirus se répand de manière exponentielle », 15 avril 2020
P. BOUCHER, « Une division de l'informatique est créée à la chancellerie « Safari » ou la chasse aux Français », *Archive le Monde*, 21 mars 1974
C. FORGET, « Protection des données dans le secteur de la « police » et de la « justice » », Février 2019
C. FERAL-SCHUHL, « Les règles générales, CNIL : une autorité de contrôle pour la France », *Cyberdroit*,, Titre 11, 2019
E. DELISLE, « Le nouveau rôle de la CNIL », *JS* 2019, n°196
L. GRARD, « Protection des données personnelles des migrants et fermeture des frontières de l'Union européenne », *Revue de l'Union européenne*, 04 septembre 2020
J. GHESTIN, « L'ordre public, notion à contenu variable », p. 77
A. DANIS-FATOME, « Ordre public et protection des données à caractère personnel », 18 septembre 2019
M. KHELOUFI, « Le droit à la protection des données à caractère personnel face au défi migratoire », *Revue de l'Union européenne*, 04 septembre 2020
W. J. MAXWELL, « La protection des données à caractère personnel aux Etats-Unis : convergences et divergences avec l'approche européenne »
R. Bellanova et P. DE HERT, « Protection des données personnelles et mesures de sécurité : vers une perspective transatlantique », 2009
A. NOIVILLE, « Valeur des données personnelles et protection des droits fondamentaux », octobre 2016
I. JOLLY, "Data protection in United States: overview, practical law", 2014/2015, p.3
S. DU PERRON, « Projet de loi 64 : une réforme à l'européenne du droit à la protection des renseignements personnels », 17 juin 2020
W MEE et E. MARSHALL et I. AHMAD, « Projet de loi fédéral sur la réforme de la protection des renseignements personnels dans le secteur privé », 24 novembre 2020
J. EYNARD, « Agence européenne chargée de la sécurité des réseaux et de l'information », *Répertoire IP/IT et Communication / Cybersécurité*, janvier 2021

Le Monde du Droit, « Cybersécurité de l'UE : la Commission propose une Unité conjointe de sécurité afin de renforcer la réaction face aux incidents de sécurité majeurs », 23 juin 2021
Le Monde, « Le nombre de plaintes à la CNIL en hausse de 27% en 2019 », publié le 09 juin 2020
Le Monde, « 204 millions d'euros d'amende pour British Airways après un vol massif de données bancaires de ses clients », publié le 08 juillet 2019

S. FABI, « Canada : vaccination obligatoire pour les passagers et les employés des compagnies aériennes », *Air Journal*, le 14 août 2021
G. Greenwald, "NSA collecting phone records of millions of Verizon customers daily", *The Guardian*, 06 Juin 2013

https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20131227trib000802909/il-y-a-100-ans-naissait-l-aviation-commerciale-et-ca-coutait-cher.html
https://www.lyonmag.com/article/110634/lyon-mona-le-nouveau-systeme-de-reconnaissance-faciale-a-l-aeroport-saint-exupery
https://www.rfi.fr/fr/emission/20151216-union-europeenne-vers-super-frontex-pouvoirs-migration-schengen
https://www.lopinion.fr/edition/international/espace-schengen-propositions-d-emmanuel-macron-reforme
https://www.usine-digitale.fr/article/l-aeroport-d-orly-teste-la-reconnaissance-faciale-a-l-embarquement-avec-la-compagnie-transavia.N1074209
https://www.ouest-france.fr/europe/ue/un-systeme-d-intelligence-artificielle-pour-garder-les-frontieres-de-l-ue
https://www.alain-bensoussan.com/avocats/cybersecuriteetrgpddeux-amendes-records-au-royaumeuni/2020/11/17/

VI. Jurisprudences

CIJ, Burkina Fasso v. République du Mali, 1986, affaire 63
CIJ, Cambodge v. Thaïlande, 1962, affaire 45
CEDH, S. et Marper c. Royaume-Uni, 04 décembre 2008, requêtes n°30562/04 et 30566/04
CJCE, 1e chambre, Nural Ziebell c/ Land Baden-Württemberg, 08 décembre 2011, n°371/08
CJCE, Commission des communautés européennes / République fédérale d'Allemagne, 09 mars 2010, affaire c-518/01
CJUE, avis 2/13 du 18 décembre 2014, point 191
CJUE, Michael Schwarz c/ Stadt Bochum, 17 octobre 2014, affaire C-291/12
CJUE, Schrems c/ Data Protection Commissionner of Ireland, 06 octobre 2015, affaire C-362/14
CJUE, Digital Rights Ireland / Steitlinger, 08 avril 2014, affaire C-293/12 et C-594/12
CJUE, Orange Romania SA c/ ANSPDCP, 11 novembre 2020, affaire C-61/19
CJUE, Data Protection Commissioner c/ Facebook Ireland and Maximillian Schrems, 16 juillet 2020, affaire C-311:18
Cass, civ. 1e, 10 septembre 2015 n°14-22.223
Cass, civ. 1ᵉ ,19 mars 2009, n°08-11617

Cass. Crim. 28 septembre 2004 pourvoi n°03-86.604
Tribunal administratif de Paris, 26 février 2019, n°1711819/3-1
CEPD, avis n°6/2015, 2015
CNIL, avis du 28 janvier 2016 délibération n°2016-012
CNIL, avis du 29 mars 2019 délibération n°2019-027
ICO Penalty Notice, British Airways, case ref. COM0783542, 16 october 2020
Supreme Court of the United States, Schmerber v. California, 20 juin 1966

VII. Rapports publics et communiqués de presse

- Rapports publics

Rapport d'information n°898 de l'Assemblée nationale sur l'Espace Schengen et la maîtrise des frontières extérieures de l'Union européenne produit par Messieurs les Députés Ludovic MENDES et Christophe NAEGELEN
Rapport spécial de 2014 de la Cour des Comptes Européenne – « Les enseignements tirés du développement par la Commission du système d'information Schengen de deuxième génération »
Rapport de la Commission du 21 décembre 2016 sur l'évaluation du Système d'Information Schengen de deuxième génération
Rapport de la Commission au Conseil et au Parlement européen du 25 novembre 2020 sur le fonctionnement du mécanisme d'évaluation et de contrôle de Schengen
Rapport de la Commission au Parlement européen et au Conseil du 29 juin 2017 sur le fonctionnement de l'agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA)
Rapport de la Commission informatique et liberté, *La documentation française*, décret n°74.938 du 08 novembre 1974
Recommandation du Conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, 23 septembre 1980
Groupe de travail « article 29 » sur la protection des données – Lignes directrices sur la transparence au sens du règlement n° (UE) 2016/679 adoptées le 29 novembre 2017
Rapport public du Conseil d'Etat, Réflexions sur l'intérêt général 1999
Rapport d'étape sur les évolutions en matière de législation sur la protection des données au Canada (2001-2007) – Rapport à la Commission européenne, mai 2017
Note d'analyse, « Les conséquences économiques d'un abandon des accords de Schengen », *France Stratégie*, Février 2016 N°39
E. BOTHOREL, Rapport d'information pour la Commission des affaires européennes de l'Assemblée nationale sur les effets de la transformation de l'agence européenne ENISA sur

l'architecture de la cybersécurité européenne et les conséquences plus larges de l'adoption du paquet cybersécurité, 25 juillet 2019
FRONTEX, Report Artificial Intelligence – Based capabilities for the European Border and Coast Guard, 21 mars 2021
Livre blanc de la Commission européenne – Intelligence artificielle, « Une approche européenne axée sur l'excellence et la confiance », 19 février 2020

- Communiqués de presse

Communication de la Commission au Parlement européen et au Conseil, « Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité », 06 avril 2016,
Communication 02/06/2021 from the Commission to the European Parliament and the Council "A strategy towards a fully functioning and resilient Schengen area"
Communiqué de presse du Conseil de l'Union européenne, « Réforme du régime d'asile européen commun : le Conseil est prêt à entamer des négociations sur Eurodac », 09 décembre 2016
Communiqué de presse du Conseil de l'Union européenne, « Système d'information sur les visas : accord provisoire entre la présidence du Conseil et le Parlement européen sur les points principaux », 08 décembre 2020
Communication de la Commission européenne au Parlement européen et au Conseil du 27 novembre 2013, « Rétablir la confiance dans les flux de données entre l'Union européenne et les Etats-Unis d'Amérique »
Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions Stratégie de cybersécurité de l'Union européenne, « Un cyberespace ouvert, sûr et sécurisé », 07 février 2013
Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 05 juillet 2016, Renforcer le système européen de cyber résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité
Communication de la Commission du 12 décembre 2006 sur un programme européen de protection des infrastructures critiques
Communiqué de presse de la Commission européenne du 23 juin 2021, « Cybersécurité de l'Union européenne : la Commission propose la création d'une unité conjointe de cybersécurité afin d'intensifier la réaction aux incidents majeurs de sécurité »
Communication conjointe au Parlement européen et au Conseil du 16 décembre 2020, « La stratégie de cybersécurité de l'UE pour la décennie numérique »

Communication de la Commission au Parlement européen, au Conseil européen, au Comité économique et social européen et au Comité des régions du 25 avril 2018, « L'intelligence artificielle pour l'Europe »

VIII. Sites internet

Site EUR-LEX : https://eur-lex.europa.eu/legal-content/
Site de la CNIL : https://www.cnil.fr/fr/
Site Vie Publique : https://www.vie-publique.fr/
Site Schengen Visa Info : https://www.schengenvisainfo.com/fr/
Site ETIAS Visa : https://www.etiasvisa.com/fr/
Site du Parlement européen : https://www.europarl.europa.eu/
Site de la Commission européenne : https://.ec.europa.eu/
Site d'Interpol : https://www.interpol.int/fr
Site de l'Elysée : https://www.elysee.fr/
Site de FRONTEX : https://frontex.europa.eu/fr/
Site d'eu-LISA : https://www.eulisa.europa.eu/
Site Toute l'Europe : https://www.touteleurope.eu/
Site de la compagnie aérienne Lufthansa : https://www.lufthansa.com/fr/
Site de la société THALES : https://www.thalesgroup.com/fr/
Site Préfecture de Lozère : https://www.lozere.gouv.fr/
Site du Contrôleur européen de la protection des données : https://edps.europa.eu/_fr
Site Youtube : https://www.youtube.com/
Site de la Federal Trade Commission : https://www.ftc.gov/
Site de l'Autorisation de Voyage Electronique : https://www.canada-ave.com/fr/
Site du gouvernement du Canada : https://www.canada.ca/fr.html
Site de l'Electronic System for Travel Authorization: https://esta.cbp.dhs.gov/
Site du Commissariat à la protection de la vie privée du Canade : https://www.priv.gc.ca/fr
Site du Bureau du vérificateur général du Canada : https://www.oag-bvg.gc.ca
Site de l'ENISA : https://www.enisa.europa.eu/
Site de l'ANSSI : https://www.ssi.gouv.fr/
Site de la société IDEMIA : https://www.idemia.com/fr
Site Aéroports de Paris : https://www.parisaeroport.fr/

IX. Autres

Reportage Cash Investigation, France 2, « Le business de la peur », 22 septembre 2015
MOOC créé par la CNIL, *Atelier RGPD*, 2021

Cartographie Le Monde de Francesca Fattori et Xemartin Laborde
Infographie de la Commisson européenne du 23 juin 2021, Joint Cyber Unit
Documents de travail du service juridique de Transavia France

TABLE DES MATIÈRES

REMERCIEMENTS **2**

GLOSSAIRE **6**

INTRODUCTION **9**

PARTIE I – LES DÉFIS DE LA SÛRETÉ ET DE LA SÉCURITÉ DES FRONTIÈRES EXTÉRIEURES EN EUROPE À SURMONTER **17**

Titre I - La nécessité d'un système électronique d'autorisation de voyage **17**

Chapitre I. La remise en cause du système actuel de l'espace Schengen 17

Section I. Les principes fondamentaux des accords de Schengen 17

I. La disparité des frontières intérieures pour un renforcement des frontières extérieures 17

II. La distinction entre les ressortissants de pays tiers soumis à visa et ceux exemptés 19

III. L'établissement et le développement du Système d'Information Schengen 21

Section II. Les difficultés de Schengen imposant la réforme en 2021 23

I. La problématique du contrôle des frontières extérieures 23

A. Le manque de coordination et de confiance mutuelle 23

B. Les efforts importants de l'Union européenne mais insuffisants 25

C. La réforme visant au sauvetage de l'acquis Schengen 27

1. La France à l'initiative de cette réforme 28

2. Rendre l'espace Schengen résilient : Stratégie Schengen 2021 29

Chapitre II. Les mutations engendrées par un système électronique d'autorisation de voyage 31

Section I. La mise en place de l'ETIAS 31

I. Un objectif justifiant le champ d'application 31

II. La structure à deux niveaux de l'ETIAS 32

A. L'unité centrale ETIAS : FRONTEX 32

1. Les limites initiales d'une agence européenne au centre de la surveillance des frontières extérieure 32

2. Des nouvelles prérogatives pour renforcer le poids de cette agence 34

B. L'unité nationale ETIAS 34

III. La procédure de délivrance d'une autorisation de voyage 35

A. L'examen de la demande 35

B. Le réexamen possible d'une autorisation de voyage délivrée 38

Section II. L'impact de l'instauration de l'ETIAS pour le transporteur aérien sur le régime français des passagers non-admissibles 38
I. L'abandon par l'Etat de ses prérogatives de puissance publique au profit d'une lourde responsabilité du transporteur aérien 38
II. La problématique épineuse de la vérification documentaire manuelle 41
A. L'accès au système d'information ETIAS par le portail des transporteurs
B. Une possible solution pour une vérification documentaire efficace 42

Titre II - Des systèmes d'information collectant un nombre grandissant de données à caractère personnel 43
Chapitre I. La solution de l'interopérabilité des systèmes d'information 43
Section I. Une collecte de données existantes par des systèmes d'information en pleine expansion 43
I. La notion de système d'information 43
II. Le fonctionnement et l'expansion des différents systèmes d'information européens 44
Section II. L'effet multiplicateur de la mise en place de l'interopérabilité 47
Chapitre II. Le rôle central et renforcé de l'agence européenne eu-LISA dans la gestion des données à caractère personnel 50
Section I. Le poids prépondérant de l'agence eu-LISA par l'élargissement de son mandat 50
I. La mise en place de l'agence européenne eu-LISA 50
II. L'élargissement de son mandat en 2017 à la vue de ses résultats satisfaisants 51
Section II. La responsabilité *de facto* croissante à l'égard des droits fondamentaux 53

PARTIE II - LES ENJEUX DU DROIT À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL FACE AUX NOUVEAUX BESOINS DE SÉCURITÉ ET D'INFORMATION 55

Titre I- La discutabilité de l'effectivité du droit à la protection des données à caractère personnel 55
Chapitre I. L'évolution des grands principes du droit à la protection des données à caractère personnel 55
Section I. Les principes attachés au traitement des données à caractère personnel 55
I. L'historique de la réglementation relative aux données à caractère personnel 55
A. Des initiatives dès les années 1970 55
B. L'harmonisation à partir de 1995 56
C. La consécration depuis 2016 57
II. Les principes fondamentaux relatifs au traitement des données à caractère personnel 58
A. Définition du traitement de données et champ d'application du RGPD 58
B. Les principes de la protection des données 59

1. Licéité du traitement 59
2. Finalité du traitement 60
3. Minimisation des données 61
4. Conservation limitée et sécuritaire des données 61
5. Protection particulière des données sensibles 62
Section II. Les droits des individus concernés et l'autorégulation 63
I. Les droits hautement protecteurs pour les individus à l'égard de leurs données à caractère personnel 63
A. Droit d'information 63
B. Droit d'accès et rectification 64
C. Droit d'opposition 65
D. Droit à l'oubli 65
II. L'existence d'autorités gardiennes du respect de ces droits 66
A. A l'échelle nationale : la Commission Nationale de l'Informatique et des Libertés 66
B. A l'échelle européenne : le Contrôleur européen de la protection des données et la Cour de Justice de l'Union européenne 69
1. Le Comité européen de la protection des données 69
2. La Cour de Justice de l'Union européenne 69
Chapitre II. Des principes et des droits confrontés à une ingérence au nom de la sécurité publique 71
Section I. La particularité d'un traitement de données au nom de l'exécution d'une mission d'intérêt public 71
I. L'étude du respect des principes attachés au traitement de données 71
II. Une ingérence possible au nom de notions floues 74
Section II. Le déséquilibre notable entre les individus et autorités nationales et européennes 75
I. L'obtention impossible d'un consentement réel 75
II. Une architecture complexe restreignant les droits des personnes 77

Titre II- Un équilibre cornélien mais politique entre protection et sécurité 79
Chapitre I. Entre approche économique et protectrice : les exemples étrangers 79
Section I. Le système américain : une approche économique 79
I. Le fonctionnement de l'autorisation électronique de voyage américaine 79
II. Régime américain de protection des données : les données personnelles comme biens marchands 80
Section II. Le système canadien : une approche protectrice 84
I. Le fonctionnement de l'autorisation électronique de voyage canadienne 84
II. Régime canadien de protection des renseignements : un niveau de protection adéquat aux normes européennes 85

Chapitre II. Le développement d'outils pour une Europe qui protège : la sécurité numérique 89
Section I. Le besoin d'une stratégie offensive de cybersécurité de l'Union européenne 89
I. La mise en place progressive d'une réglementation européenne pour faire face aux nouvelles menaces sophistiquées 89
A. Une prise de conscience tardive.....89
B. Une accélération nécessaire en 2020.....90
C. Le soutien financier de l'Union européenne 92
II. L'établissement et le développement d'acteurs impliqués dans la cybersécurité ...93
A. A l'échelle européenne : Agence européenne chargée de la sécurité des réseaux et de l'information.....93
B. A l'échelle nationale : Agence nationale de la sécurité des systèmes d'information 94
Section II. Vers une sécurité organisée autour de l'intelligence artificielle 94
I. L'élaboration d'un cadre juridique européen sur l'intelligence artificielle.....95
II. L'application de l'intelligence artificielle dans la gestion de la migration et le contrôle aux frontières.....97
A. L'utilisation de la reconnaissance faciale dans la gestion des frontières françaises 97
B. Le détecteur de mensonge aux portes des frontières françaises : iBorderCtrl.....99

CONCLUSION.....101

BIBLIOGRAPHIE.....103

TABLE DES MATIÈRES 116

RÉSUMÉ

Mai 2022 marquera l'instauration de l'autorisation électronique de voyage en Europe : l'ETIAS. Son ambition est d'accroître le niveau de sécurité et de sûreté dans l'espace Schengen afin de remédier aux nombreuses problématiques rencontrées par les Etats membres. Selon eux, ce défaut sécuritaire est intimement lié au défaut d'information qu'a l'Union européenne sur ses migrants. Pour y remédier, l'Union met en place l'interopérabilité de divers systèmes d'information qui collectent et opèrent un grand nombre de traitements de données à caractère personnel. Or, le Règlement Général sur la Protection des Données de 2016 assure un niveau élevé de protection des données personnelles et garantit des droits hautement protecteurs pour les personnes concernées. L'instauration de cette autorisation de voyage peut poser question sur une remise en cause du RGPD, sur la conciliation des principes découlant de ce texte et les défis auxquels les Etats doivent faire face pour assurer des niveaux de sûreté et de sécurité élevés. La protection et la sécurité peuvent-elles être conciliables ou bien la pratique démontre-t-elle la nécessité de faire un choix ?

Mots-clefs : Données personnelles / Schengen / Système d'information / Sécurité / Sûreté / ETIAS

SUMMARY

May 2022 will mark the introduction of the Electronic Travel Information Authorization System in Europe: ETIAS. Its ambition is to increase the level of security and safety in the Schengen area in order to remedy the numerous problems encountered by the Member States. According to them, this lack of security is closely linked to the lack of information that the European Union has on its migrants. To remedy this, the Union is implementing the interoperability of various information systems that collect and operate a considerable amount of personal data processing. However, the General Data Protection Regulation of 2016 ensures a high level of protection of personal data and guarantees highly protective rights for the persons concerned. The introduction of this travel authorisation may raise questions about the GDPR, about the conciliation of the principles deriving from this text and the challenges that States must face to ensure a high level of safety and security. Can protection and security be reconciled or does practice demonstrate the need to make a choice?

Keywords: Personal data / Schengen / Information system / Security / Safety / ETIAS