LA RECONNAISSANCE FACIALE

Mémoire de recherche pour l'obtention du Master 2 Droit et Management du Transport Aérien

par
Abdullah SEN

Sous la direction de M. Jean-François GUITARD

Pôle Transports
Aix*Marseille Université
CDMT · IFURTA
Faculté de Droit et de Science Politique

Année universitaire 2018-2019
3 AVENUE ROBERT SCHUMAN – 13623 AIX EN PROVENCE CEDEX 1

Aix-Marseille Université
Faculté de droit et science politique

Pôle Transports
Institut de Formation Universitaire et de Recherche du Transport Aérien

La Reconnaissance Faciale

Mémoire pour l'obtention du Master 2 Droit et Management du Transport Aérien

par

Abdullah SEN

Sous la direction de Mr. Jean François GUITARD

Année universitaire 2018-2019

« La meilleure chose que l'on puisse dire pour l'instant c'est de continuer à observer l'environnement.
Et s'attendre à ce que l'environnement nous observe de plus en plus en retour. »

Citation du journaliste Luke Dormehl, en date du 13 mai 2019.

Remerciements

Avant d'entamer le développement de mon mémoire, je souhaite remercier toutes les personnes qui ont contribué au succès de mon alternance et qui m'ont aidé lors de la rédaction de ce mémoire.

Tout d'abord, j'adresse mes remerciements au directeur du Pôle Transport, Mr le Professeur Cyril BLOCH ainsi qu'à notre directrice de master, Mme Julie LABORDE dit BOURIAT de l'Université d'Aix-Marseille.

Je tiens, ensuite, à remercier tout particulièrement mon maître d'apprentissage, Mr. Maximilien SCHOLLHAMMER, responsable sûreté et qualité au sein de l'EuroAirport Bâle-Mulhouse pour son accueil, sa confiance et le partage de son expérience au quotidien. Le thème du mémoire qu'il a choisi m'a permis de mieux cerner les enjeux des nouvelles technologies de l'identification et de participer plus activement aux travaux liés au système de reconnaissance faciale installé au sein de l'aéroport. Je remercie également toute l'équipe du service sûreté et qualité de l'EuroAirport ainsi que les collègues des autres services qui m'ont aidé dans la rédaction de ce mémoire.

Je remercie également M. Jean-François GUITARD, mon directeur de mémoire, pour avoir porté un intérêt particulier à mon mémoire et ses conseils sur les aspects pratiques de ce thème.

Enfin, je tiens à remercier ma mère et mon père pour leur soutien sans faille et les valeurs qu'ils m'ont transmises. Je remercie également mes sœurs et mes amis pour leur soutien pendant la rédaction de ce mémoire.

Sommaire

Table des abréviations et sigles utilisés

AFEA	*Automated Face Expression Analysis*
ADN	Acide désoxyribonucléique
ADP	Aéroport de Paris
BIPA	*Biometric Information Privacy Act*
CBP	*Custom and Border Protection*
CEDH	Cour européenne des droits de l'Homme
CEPD	Contrôleur européen de la protection des données
CJUE	Cour de Justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
Conv. EDH	Convention européenne des droits de l'Homme
DARPA	*Defense Advanced Research Projects Agency*
DHS	*Department of Homeland Security*
DVLM	Document de voyage lisible à la machine
EBGM	*Elastic Bunch Graph Matching*
ENISA	*European Network and Intelligence Security Agency*
FAR	*False Acceptance Rate*
FBI	*Federal Bureau of Investigation*
FRR	*False Rejection Rate*
FRVT	*Face Recognition Vendor Test*
IBIA	*International Biometric Industry Association*
ISO	*International Standardisation Organisation*
KTDI	*Known Traveler Digital Identity*
LDA	*Linear Discriminant Analysis*
NIST	*National Institute of Standards and Technologies*
OACI	Organisation de l'aviation civile internationale
PCA	*Principal Component Analysis*
PARIF	Passage à accès routier d'inspection filtrage
PIF	Poste d'inspection filtrage
TSA	*Transportation Security Administration*
RGPD	Règlement général sur la protection des données.
ZSAR	Zone de sûreté à accès réglementé

Introduction

En 1948, l'écrivain George Orwell imaginait dans son roman intitulé « 1984 » une société totalitaire dans laquelle tous les citoyens sont observés et surveillés par le « *Big Brother* ». Chaque individu est suivi de très près par les caméras et sont sanctionnés en fonction de leurs agissements, voire de leurs pensées. Imagination ou révélation, ce que l'auteur décrit dans son livre est aujourd'hui au cœur des débats dans nos sociétés. Alex Türk, l'ancien directeur de la Commission nationale de l'informatique et des libertés (CNIL), estime que « *nous vivrons tous, à l'horizon 2020, dans une société dans laquelle il sera impossible de travailler, de se divertir, de se déplacer, de vivre donc, sans être tracés*[1] ».

La reconnaissance faciale joue un rôle central dans ce débat, notamment par sa présence envahissante dans les zones publiques comme les aéroports. Compte tenu des attaques terroristes qui impliquent les aéroports comme celles à Istanbul et Bruxelles en 2016 ou encore à Orly en 2017, les pouvoir publiques font appel à des mesures biométriques pour reconnaître et neutraliser les terroristes. Mais ce discours sécuritaire soulève des questions notamment par rapport au respect de la vie privée et des droits fondamentaux. Au long de cette étude, nous essaierons donc de répondre à la question suivante : l'utilisation de la reconnaissance faciale est-elle une solution adéquate face aux menaces qui pèsent sur la société, plus particulièrement sur les aéroports ?

Avant d'analyser le rôle de cette technologie, il est nécessaire de prendre du recul et de détailler certaines notions clés qui gravitent autour d'elle. Dans cette introduction nous concentrerons la réflexion dans un premier temps sur ce que représentent les données personnelles et la biométrie en essayant de démontrer qu'il existe un lien entre les deux concepts (I) mais ce lien varie en fonction des conceptions sur les données personnelles. Puis dans un deuxième temps, nous nous focaliserons sur la naissance accélérée de la reconnaissance faciale (II) en rappelant son histoire et en définissant les notions qui relèvent de vocabulaire technique afin de mieux comprendre les enjeux de cette technologie. Enfin, nous évoquerons les risques liés à la banalisation de la

[1] N. Véron, *Le contrôle de l'utilisation des données biométriques au regard du droit au respect de la vie privée* (p. 15)

reconnaissance faciale (III), qui est aujourd'hui une technologie indispensable dans le quotidien des individus.

I. Comprendre le lien entre les données personnelles et la biométrie.

Les avancées dans le domaine des nouvelles technologies de l'information et de la communication (NTIC) permettent aux autorités, aux entreprises et aux individus de suivre le comportement d'autres personnes sans qu'elles en soient informées. En effet les données qui découlent de l'utilisation des outils des NTIC peuvent être collectées par n'importe qui (ou presque) permettant ainsi de suivre le comportement de chacun. Cette volonté de « suivre » est apparue dans les années 1980 avec le courant néolibéral, comme le souligne Kelly A. Gates dans son ouvrage. Elle estime que les néolibéraux ont accéléré le processus de la biométrie, sachant que ce sont les banques qui ont été les premières à utiliser la technologie biométrique[2].

Ce suivi des personnes se base sur des « traces » laissées par les utilisateurs des NTIC. On entend ici par traces à la fois les données numériques qui se créent à chaque navigation sur Internet, mais également les données biométriques qui sont propres à chaque individu comme les empreintes digitales ou encore le visage. Ces deux types de données composent ce que l'on appelle communément les données personnelles.

1.1. Qu'est-ce qu'une donnée biométrique ?

La CNIL définit la biométrie sur son site internet[3] comme étant « *l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.* » Elle confirme par la suite que ces données-là sont « *des données à caractère personnel car elles permettent d'identifier une personne* ». L'empreinte biométrique est une donnée personnelle permettant d'identifier ou de reconnaître un individu avec des outils de biométrie. En France, c'est depuis la loi du 6 août 2004 ayant modifié la loi n° 78-14 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés que le terme de « données biométriques » apparaît explicitement. Donc lorsqu'une image du visage est

[2] K. A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance (Critical Cultural Communication)*, p.38
[3] https://www.cnil.fr/fr/definition/biometrie

prise ou une empreinte digitale est prélevée, on crée une d'empreinte biométrique qui sera stockée dans une base de données.

La particularité d'une donnée biométrique c'est qu'elle présente trois caractéristiques : elle est universelle (présente chez tout individu), unique (propre à chacun) et permanente. On subdivise généralement la biométrie en deux parties, il y a d'un côté la biométrie avec trace utilisable à l'insu de la personne (empreinte digitale) et de l'autre côté la biométrie sans trace qui est plus difficile à compromettre (réseau veineux du doigt). Cependant, le visage s'inscrit dans une catégorie intermédiaire, puisqu'en soi il ne laisse pas de trace mais l'utilisation d'un système de vidéosurveillance peut conduire à un résultat similaire car notre visage filmé crée des traces numériques, d'autant plus que le visage d'un individu peut être capté à son insu. Comme le précise Pierre Piazza « *la technologie biométrique consiste en somme à transformer certaines caractéristiques physiques ou physiologiques propres à une personne en une empreinte numérique exploitable informatiquement afin d'être à même de savoir qui est qui avec une quasi-certitude* »[4].

1.2. L'affirmation du caractère personnel des données biométriques.

La Cour européenne des droits de l'Homme (CEDH) s'est prononcée dans le sens de la CNIL en considérant les données biométriques comme des données personnelles. Elle l'a affirmée de manière solennelle dans sa décision du 4 décembre 2008, S. et Marper contre Royaume-Uni. En l'espèce, il s'agissait d'une affaire où les autorités britanniques conservaient les données ADN de toutes les personnes étant entrées en contact avec les forces de l'ordre, même en l'absence d'une condamnation. De plus, ces données étaient conservées pour une durée illimitée afin de constituer une base de donnée dont pourrait se prévaloir les autorités britanniques à l'avenir[5]. La CEDH s'est opposée à cette pratique car contraire aux dispositions de l'article 8 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de du 28 janvier 1981.

[4] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 19 par P. Piazza, *Les résistances à la biométrie en France*, §2

[5] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 3 par S. A. Cole, *La saisie de l'ADN aux États-Unis et au Royaume-Uni à des fins d'identification des individus : origines et enjeux*, §16

Les données personnelles suscitent aujourd'hui un intérêt particulier pour les entreprises, notamment les entreprises que l'on considère comme « les géants du Web » appelées aussi les GAFAM (acronyme pour les compagnies suivantes : Google, Apple, Facebook, Amazon et Microsoft). Ces entreprises internationales utilisent les données de leurs utilisateurs afin d'en tirer un profit économique. Les « traces » numériques laissées par un individu sur Internet permettent aussi de connaître l'identité d'une personne. Afin d'encadrer l'utilisation des données personnelles, l'Union européenne avait adopté dans un premier temps une directive le 24 octobre 1995 (95/46/CE) sur la protection des données personnelle. Dans son article 28, cette directive prévoit une protection des données personnelles confiée aux autorités nationales de protection de données, et institue dans son article 29 le Groupe de travail (G29) qui regroupe toutes les autorités de protection des données personnelles des Etats Membres de l'Union européenne. Depuis l'entrée en vigueur du RGPD, le G29 est remplacé par le Comité européen de la protection des données qui veille à l'application uniforme des dispositions du RGPD.

Le règlement CE 45/2001 a mis en place le Contrôleur européen de la protection des données (CEPD) qui supervise notamment les échanges de données entre les institutions de l'Unions européenne et veille au respect à la vie privée des individus. Aujourd'hui pour harmoniser les législations des Etats membres, c'est le Règlement général sur la protection des données (règlement n°2016/679) qui est applicable depuis le 25 mai 2018 remplaçant ainsi la directive du 24 octobre 1995. En outre, ce nouveau texte donne des prérogatives de sanction aux autorités nationales de protection des données personnelles, comme la CNIL, qui peuvent infliger des amendes très lourdes en cas d'infraction. Ainsi le montant d'une amende peut s'élever à 20 Millions d'euros ou dans le cas d'une entreprise à 4% du chiffre d'affaire annuel mondial[6]. De plus, l'activité litigieuse peut également être suspendue en cas de manquement au RGPD. Néanmoins, le texte supprime les contrôles a priori effectués par les autorités nationales de protection des données.

[6] https://www.cnil.fr/fr/definition/sanction

1.3. Une protection variable des données personnelles au niveau mondiale

Du côté de l'Europe, les données personnelles sont protégées car elles sont considérées comme des attributs de la personne. Outre Atlantique, la conception des données personnelles est différente, puisqu'aux Etats-Unis elles sont considérées comme une valeur marchande régie par les règles du marché. C'est ce qui explique notamment l'absence d'autorité fédérale de protection des données personnelles ou encore de règles fédérales de protection des données[7] semblables au RGPD. Il existe toutefois un texte, le « *Privacy Act* » de 1974, mais il encadre l'utilisation des données personnelles détenues par l'administration fédérale, et ne se prononce pas sur l'utilisation faite par les personnes privées ou les Etats fédérés. C'est pourquoi, la justice américaine joue un rôle plus actif dans ce domaine. Selon la jurisprudence américaine, les citoyens américains bénéficient « d'une attente raisonnable envers le respect de la vie privée[8] », mais ceci n'est pas équivalent au respect du droit à la vie privée car la conception américaine estime que les citoyens qui révèlent des informations en public, tel que leur visage par exemple, ne peuvent bénéficier d'un droit à l'intimité de cette information.

L'unique protection dont bénéficient les américains découle du 4ème Amendement de la Constitution des Etats-Unis qui interdit les perquisitions et saisies non motivées. Néanmoins, l'utilisation d'une caméra qui augmente les capacités humaines de perception en prenant une photo ne contredit pas ce texte. C'est également ce qui explique le choix lexical de la part des gestionnaires de base de données ADN qui utilise le terme de « *sampling* » (échantillonnage) au lieu des termes de « *seizure* » (prise/saisie) lorsqu'il s'agit d'un prélèvement de matériel génétique sur les personnes[9].

Dans une affaire, « *Davis v Mississipi* » de 1969, les juges de la Cour suprême ont annulé la condamnation de John Davis prononcée suite au prélèvement de ses empreintes digitales lors d'une intervention qui ciblait les jeunes afro-américains de la ville. Cette annulation touche à la détention sans motif valable de John Davis et non au

[7] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* – Chapitre 5 *Les technologies identitaires biométriques : que fait l'Europe face aux États-Unis ?* par B. DIDIER et C. PELLEGRINO, §13.
[8] Katz v United States, 1967 « *Reasonable expectation to privacy* » – Dow Chemical Co v United States, 1986
[9] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 3 par S. A. Cole, *La saisie de l'ADN aux États-Unis et au Royaume-Uni à des fins d'identification des individus : origines et enjeux*, §3

prélèvement de ses empreintes, ce qui renforce ainsi l'idée selon laquelle les prises d'empreintes ne sont pas des saisies illégales au sens du 4e Amendement. Une autre décision de la Cour suprême semble fixer une limite à la méthode de prélèvement utilisée. En effet, dans la décision « *Kyllo v United States* » en date de 2001, les juges ont déclaré que l'utilisation d'une caméra thermique pour espionner un suspect est contraire au 4e Amendement, parce que cette technologie n'est pas disponible au public. Toutefois, cette décision ne produit presque aucun effet aujourd'hui puisque l'utilisation des technologies de biométrie faciale sont à la portée de tout individu.

Les Etats-Unis ont privilégié pendant longtemps une autorégulation par les industriels, mais les mesures furent inexistantes en l'absence d'une contrainte législative. En ce sens, Jonathan Philips, un des Program Manager du DARPA a même estimé que « *tant que l'Etat n'impose aucune restriction, les industriels ne sont pas tenus de fournir des pratiques et procédures de sécurité pour la protection des données privées*[10] ». Face à cela, certains Etats fédérés ont pris le pas et ont adopté des mesures sur la protection des données personnelles ainsi que sur le respect du droit à la vie privée. En ce sens, la Californie a été le premier Etat à considérer le droit à la vie privée comme un droit inaliénable comme le prévoit l'article 1e section 1 de sa Constitution :

« *All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.* »[11]

La république de Californie entend faire prévaloir le respect à la vie privée dans le domaine biométrique puisqu'elle a adopté très tôt une mesure de restriction de l'utilisation de la reconnaissance faciale. Elle a voté en 2001 le « *Senate Bill 169 »* pour réguler l'utilisation des systèmes de reconnaissance faciale notamment en imposant une notice d'information claire et concise avant le prélèvement de l'image et un consentement explicite de la personne photographiée pour autoriser le partage de sa donnée biométrique. Cette règle interdit par ailleurs la création d'une base de données permettant d'identifier les citoyens innocents. L'utilisation de la reconnaissance faciale

[10] D. McCormack, *« Can Corporate America secure our nation ? An analysis of the Identix Framework for the regulation and use of facial recognition technology »,* p.20

[11] « *Tout individu est libre et indépendant par nature et dispose de droits inaliénables. Parmi lesquels figure la liberté, le droit à la vie, la propriété, la sécurité, la quête du bonheur et la vie privée* ».

doit être raisonnablement nécessaire pour protéger la sécurité publique, la propriété privée ou contre toute violation de la loi.[12]

Dans le même sens, l'Illinois a adopté en 2008 la « *Biometric Information Privacy Act* » (BIPA) pour réguler l'utilisation des données biométriques. En outre, cette mesure impose notamment à la personne privée d'avoir une politique de confidentialité écrite, accessible au public, précisant la durée de rétention de la donnée biométrique et prévoyant sa destruction au moment de la satisfaction du besoin pour lequel elle a été prélevée ou après trois ans à compter de la dernière interaction avec l'individu concerné. De plus, lorsque la donnée est prélevée, l'individu doit être informé de l'opération de prélèvement, être averti de la finalité et durée de conservation de la donnée et fournir un consentement écrit. Enfin, la donnée biométrique ne peut être cédée ou partagée à moins que l'individu ait consenti explicitement, la seule exception prévue est le partage de données pour l'application de la loi[13].

D'autres Etats comme le Texas et le Washington ont suivi cette tendance et ont également adopté un BIPA. Ce mouvement semble se propager davantage puisque l'Alaska, le Connecticut, le Montana et le New Hampshire se penchent sur une législation encadrant l'utilisation de la biométrie. Il convient de préciser que le BIPA ne prévoit pas la mise en place d'une autorité de protection des données personnelles comme en Europe, il revient donc aux citoyens de faire valoir leur droit devant une Cour de Justice. La différence dans le traitement des données personnelles entre les Etats-Unis et l'Union Européenne semble donc se réduire.

1.4. Une industrie biométrique en forte croissance

Aujourd'hui la biométrie est en plein essor, les rapports de Markets & Markets[14] estiment que la valeur du marché de la biométrie représentait 12 milliards de dollar en 2016. Ainsi depuis 2009, le chiffre d'affaire mondial de la biométrie aurait augmenté de plus de 300%[15]. Les marchés gouvernementaux sont les moteurs du développement de l'industrie biométrique. Les grands acteurs privés de ce marché sont surtout

[12] D. McCormack, *« Can Corporate America secure our nation ? An analysis of the Identix Framework for the regulation and use of facial recognition technology »,* p.18
[13] Loi de l'Illinois 740 ILCS 14/15, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57%20
[14] https://www.businesscoot.com/fr/page/le-marche-de-la-biometrie
[15] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses – Chapitre 4 La biométrie : un secteur rentable soutenu par la commande publique,* N. Lalam et F. Nadaud, §6

européens avec des sociétés comme Gemalto (rachetée par le groupe Thalès), Oberthur, Sagem, Giesieck+Devrient et IDEMIA qui a racheté l'américain L-1 Identity Solution (issue de la fusion entre Viisage et Identix). Du côté des américains on retrouve des grandes entreprises comme Northrop Grumman et Lockeed Martin. Si les pouvoir publics sont le moteur de cette industrie, cela s'explique par l'avantage de la biométrie qui *« a pour caractéristique de relier un certain nombre de problématiques comme l'identification des individus, le contrôle de l'immigration, la lutte contre le terrorisme, le confort, l'intelligence ambiante dont la caractéristique la plus saillante et de ne pas être a priori interconnectées* » nous dit Ayse Ceyhan[16]. Il est intéressant de souligner que la multiplicité des acteurs permet d'éviter une situation de monopole.

L'OACI est aussi un acteur déterminant pour la biométrie depuis les années 1990. Pour promouvoir l'utilisation de la biométrie, notamment dans les passeports, l'OACI faisait référence aux normes biométriques du FBI et du NIST. Par la suite elle s'est tournée vers un comité ISO/EIC, c'est de là qu'a été créé le sous-comité 37 (SC 37) pour la normalisation internationale de la biométrie. Ainsi dans le DOC 9303 – DVLM, l'OACI a imposé des normes mondiales aux États pour que des données biométriques (images faciales et empreintes digitales) soient intégrées dans les documents de voyage. C'est ce qui a conduit à l'adoption du règlement européen du 13 décembre 2004 relatif à la modernisation des passeports qui invite la Commission européenne à prendre d'urgence des mesures pour renforcer la sécurité des documents et lutter contre le terrorisme[17].

II. La genèse accélérée de la reconnaissance faciale

La reconnaissance faciale est sans doute la technologie à l'épicentre du débat sur le droit au respect à la vie privée car elle suscite des inquiétudes vis à vis des risques liés à la mauvaise utilisation de cette technologie. Moins intrusive et plus discrète que l'empreinte digitale, elle fait l'objet de toutes les théories diverses et variées.

[16] A.Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 20, *« Acceptabilité » de la biométrie : linéaments d'un cadre analytique,* §6

[17] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses – Chapitre 11 : le projet INES aboutira-t-il ? par C. Lacouette Fougere*

Aujourd'hui, le marché de la reconnaissance faciale est estimé à 4.5 Milliards d'euros et devrait connaître une croissance de 10% par an d'ici 2026[18]

2.1. L'apparition de la reconnaissance faciale.

En France, le visage a été utilisé comme outil d'identification assez tôt puisque dès 1780 les passeports et les formulaires de police comportaient des indications portant sur le visage comme la couleur des yeux, la couleur des cheveux, la forme du nez et les sourcils[19]. Contrairement à l'empreinte digitale, la reconnaissance faciale est « *user friendly*[20] » car ne nécessite pas forcément de coopération. La reconnaissance faciale, selon la CNIL, « *est une technique qui permet à partir des traits de visage soit d'authentifier une personne : c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès) soit 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* »[21].

Dans les années 1960, les scientifiques ont développé des algorithmes de détection des visages dans une image et des algorithmes pour distinguer deux visages[22]. Toutefois, la commercialisation de la technologie n'a débuté concrètement que dans les années 1990 avec des entreprises américaines comme Visionics, Viisage et Miros Inc. A l'instar des autres outils de la sécurité et de l'identification, la reconnaissance faciale a été fortement accélérée par les attentats du 11 septembre 2001 à New York.

Une anecdote vaut la peine d'être mentionnée ici : en juin 2001, c'est à dire au moment de l'adoption de la SB 169 en Californie, William Wilson, président de l'« *International Biometric Industry Association* » (IBIA), écrit une lettre au législateur californien pour le mettre en garde sur les conséquences d'une restriction de l'utilisation de la reconnaissance faciale en indiquant notamment que les autorités ne

[18] Les Echos, *Reconnaissance faciale : comment ça marche et pourquoi ça inquiète*, https://www.youtube.com/watch?v=acYXeFSGYuA&t=29s
[19] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses – Chapitre 1 Identifier par le corps avant la biométrie aux xive-xixe siècles* par V. Denis, §8
[20] Facile d'utilisation
[21] https://www.cnil.fr/fr/definition/reconnaissance-faciale
[22] K. A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance (Critical Cultural Communication)*, p. 12

pourraient pas arrêtées une attaque perpétrée par Al Qaïda sur le territoire américain[23]. Par la suite, les images de la caméra de vidéosurveillance de l'aéroport de Portland vont faire le tour du monde et un sentiment de « technostalgie[24] » s'installera dans l'opinion publique.

Figure 1: Image issue de la caméra de surveillance de l'aéroport de Portland au matin des attaques du 11 septembre 2001. On aperçoit les deux hijackers présumés du Vol 11 de l'American Airlines.

2.2. Le développement des systèmes de reconnaissance faciale en laboratoire.

La technologie de reconnaissance faciale existait déjà avant 2001, mais du fait de ses performances médiocres, son utilisation n'intéressait pas les autorités. Le NIST effectue régulièrement des tests sur la reconnaissance faciale depuis la fin des années 1990. Ce sont principalement les producteurs de système de reconnaissance faciale qui participent à ces tests et seulement cinq compagnies étaient présentes au FRVT en 2000 dont *Visionics*, *eTrue* (anciennement Miros), *Lau Technologies*, *C-Vis Computer Vision und Automation GmbH* et *Banque-Tec International Pty Limited*. Plusieurs organismes sponsorisent ces tests comme le FBI ou encore le DARPA. Après les attentats du 11 septembre, le FRVT 2002 portait une importance plus symbolique et était d'une ampleur plus grande que les précédents car 37 437 personnes ont été enrôlées dans la base de données.

[23] Anecdote rapporté par D. McCormack*, « Can Corporate America secure our nation ? An analysis of the Identix Framework for the regulation and use of facial recognition technology »,* p.1

[24] K. A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance (Critical Cultural Communication* : « Terme employé par Pat Gill, la technostalgie est le désir d'altérer le passé par les technologies pour redéfinir le présent en utilisant la technologie à des fins humanitaires toute en étant conscient de l'impossibilité d'une telle action », p.2

Les résultats variaient en fonction de plusieurs facteurs comme l'environnement, l'éclairage, l'ancienneté de la photo et la taille de la base de donnée. Ainsi le système de reconnaissance faciale le plus performant a obtenu un taux de réussite de 85% pour une base de donnée de 800 personnes tandis que le même système obtenait un taux de réussite de 73% pour une base de donnée de 37 437 personnes.

Quatre ans plus tard, en 2006, un autre FRVT est conduit et cette fois les résultats sont plus prometteurs pour différentes raisons : la caméra utilisée pour analyser le visage ainsi que les images enrôlées dans la base de données présentaient une meilleure qualité. Par la suite d'autres tests seront effectués avec des résultats en constante amélioration.
Le graphique ci-après reprend les résultats de ces tests avec la taille de la base de données utilisée :

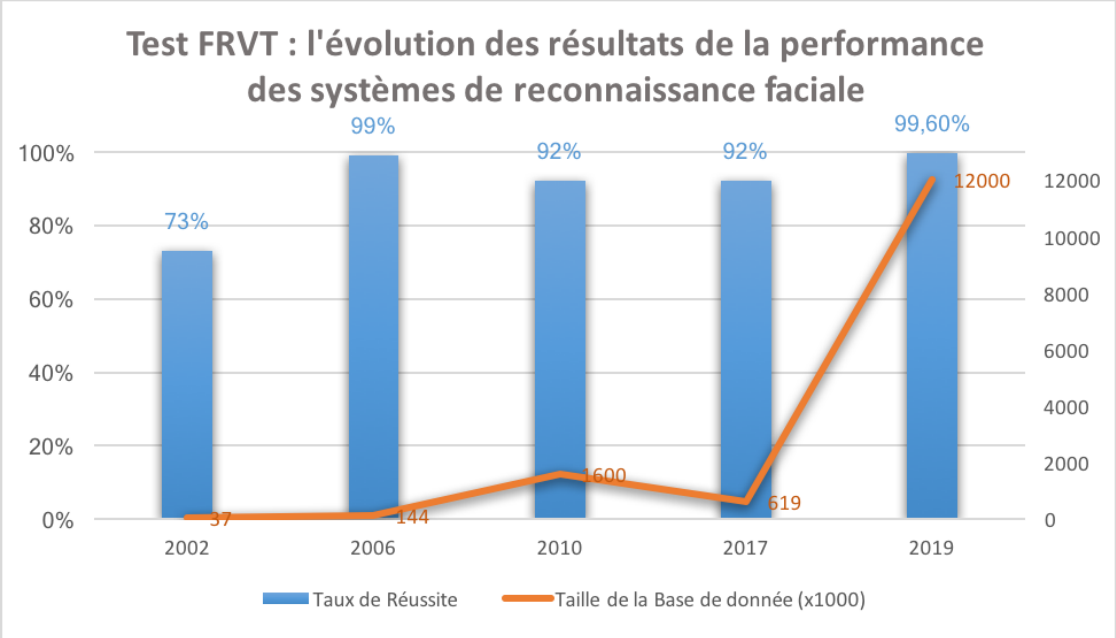

Figure 2 : L'évolution des résultats de la performances des systèmes de reconnaissance faciale. Graphique réalisé à l'aide des données du site internet de la Nationale Institute of Standards and Technologies (www.nist.gov)

En 2019, sur les 16 algorithmes qui ont été retenus pour l'identification avec une base de données de douze millions d'images, seul deux ont été en dessous de 98% (1toN). L'augmentation exponentielle de la taille des bases de données permet de se rapprocher des conditions d'utilisation opérationnelle de la reconnaissance faciale.

2.3. L'utilisation opérationnelle de la reconnaissance faciale.

Dans la pratique, la reconnaissance faciale est utilisée dans deux cas de figure de la manière suivante :

Pour l'identification, qui permet de retrouver un individu au milieu d'une foule, il est nécessaire d'effectuer un enrôlement premièrement, c'est à dire enregistrer l'image d'une personne dans une base de données. Ensuite, il faut que la personne passe devant la caméra qui va capturer son visage. Cette image est ensuite comparée avec celles présentes dans la base de données, que l'on appelle des « *template* » (gabarit). Il s'agit là d'une comparaison 1-to-N. À ce moment, si un gabarit de la base de données présente des points de similitudes élevées conduisant à un « *hit* » (rapprochement) alors la caméra identifie la personne correctement. En d'autres termes, le système de reconnaissance faciale va rechercher dans sa base de données l'image qui présente le plus de point commun avec l'image prise par la caméra.

Pour l'authentification, il s'agit d'effectuer une comparaison 1-to-1 où la personne présente un titre d'accès, tel qu'un badge, contenant son empreinte biométrique (l'image du visage). La caméra compare cette donnée biométrique avec le visage qu'elle va capturer. La personne va être authentifier si les deux images présentent des points de similitudes suffisantes.

Le seuil à partir duquel la correspondance est acceptée est défini par l'exploitant du système de reconnaissance faciale, donc si ce dernier met en place un score élevé pour valider la reconnaissance alors il réduit le taux de fausses acceptations (FAR). Si un score faible est retenu, alors le système d'identification sera plus souple mais il réduirait le taux de faux rejets (FRR). La fausse acceptation est la situation dans laquelle la caméra authentifie/identifie une personne comme faisant partie de la base de données alors qu'elle n'y figure pas. Quant aux faux rejets, c'est la situation dans laquelle le système ne parvient pas à identifier/authentifier une personne qui figure bien dans la base de données. Mais cette deuxième hypothèse présente moins de risques car un agent est présent pour remédier à ce type d'erreur. Les deux taux sont liés par l'équation suivante : FAR+FRR=1. Les autorités et autres utilisateurs de la reconnaissance faciale privilégient en général un FAR faible, l'exigence pour les

aéroports et les zones sensibles en générale se situe à environ 0.0001%. En 2006, lors des FRVT le FAR était élevé avec un taux de 0.01%[25]. Lors du FRVT de 2017, le meilleur algorithme a atteint un taux de FAR de 0.000001%.

Il existe également des individus dont il est impossible d'effectuer l'enrôlement, ils font partie de ce qu'on appelle *Failure to enrol* (FTE) et des personnes où on peut acquérir la modalité mais le traitement d'image n'est pas suffisant pour obtenir une information pouvant vérifier l'identité et c'est ce qu'on appelle le *Failure to authenticate* (FTA).

2.4. Les méthodes de détection du visage utilisées pour la reconnaissance faciale

Les méthodes traditionnelles de reconnaissance faciale se focalisent sur les yeux ou la couleur de peau. Elles adoptent soit une approche géométrique qui calcule l'espace entre les traits du visage, soit une approche photométrique qui interprète le visage comme une combinaison de visage standardisé ou une approche qui se base sur la peau en « cartographiant » la texture unique du visage de chaque individu. Pour exécuter ces techniques plusieurs algorithmes sont utilisés dans les systèmes de reconnaissance faciale mais les principaux sont les suivants :

- *Principal Component Analysis* (PCA) : il identifie le visage à partir du trait qui varie le plus au sein du visage (Eigenfaces). Cette méthode est sensible à la variation d'échelle de l'image.
- *Linear Discriminant Analysis* (LDA) : approche statistique comme la PCA et classifie les visages par rapport aux visages déjà connus. Ainsi, cette technique trouve le vecteur qui maximise les variances entre individus et minimise les variances entres les différentes images d'une même personne. Donc plus il y'a d'image plus elle sera performante.
- *Elastic Bunch Graph Matching* (EBGM) : contrairement au PCA et LDA, cet algorithme repose sur des caractéristiques non linéaires comme l'expression du visage, l'illumination ou la pose.

[25] https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51131 , p.5

L'image prise par la caméra est « normalisée » par l'algorithme c'est à dire standardisée en terme de qualité, pose et illumination pour un traitement plus efficace. La technologie a connu une révolution en 2016-2017 en basculant sur les réseaux de neurones et les performances ont été améliorées par un facteur de 40. Les réseaux de neurones sont des systèmes qui s'inspirent des neurones humains et permettent aux machines d'apprendre par eux-mêmes et de mémoriser avec les exercices à répétition.

Il faut voir la reconnaissance faciale comme un système comportant à la fois la caméra et son entretien mais aussi l'agent en charge qui doit être formé correctement pour son utilisation, donc même si des outils respectant la vie privée (*privacy by design*) sont construits ils n'empêcheront pas le détournement de finalité (*function creep*) qui repose sur le facteur humain.

Il convient également de choisir ce qui convient le mieux entre des systèmes de biométrie à « lien fort » ou « lien faible »[26] : le premier permet d'identifier un fraudeur, alors que le second ne fait que détecter la fraude. Le développement de la technologie de reconnaissance faciale a logiquement conduit à sa démocratisation avec une diffusion globale notamment grâce aux smartphones. Cette banalisation de la technologie accroît aussi les risques d'atteinte aux données personnelles des individus.

III. Les risques inhérents à l'utilisation répandue de la reconnaissance faciale.

La première utilisation de la reconnaissance faciale pour retrouver des délinquants a été lancée par l'Angleterre dans les quartiers difficiles de Londres en 1998[27]. Les autorités anglaises ont combiné le logiciel *FaceIt* avec les 300 caméras de surveillance déjà présentes, réduisant ainsi le taux de criminalité du quartier de 34%. Aujourd'hui, la reconnaissance faciale est utilisée quotidiennement par les individus et son immixtion dans la vie privée peut être graduelle. Par exemple lorsqu'elle est utilisée pour compter le nombre d'individu, aucune donnée personnelle n'est stockée ni utilisée pour d'autres fins. Lorsqu'elle est utilisée pour un ciblage, une base de donnée se construit pour proposer des publicités sur mesure en fonction du comportement de l'individu et de son âge par exemple. Enfin lorsqu'elle sert à l'identification, cela veut

[26] N. Véron, *Le contrôle de l'utilisation des données biométriques au regard du droit au respect de la vie privée* (p.169)

[27] D. McCormack*, « Can Corporate America secure our nation ? An analysis of the Identix Framework for the regulation and use of facial recognition technology »,* p.5

dire que l'on a accès à toutes les données personnelles d'un individu (adresse, nationalité, date de naissance).

L'élément le plus important dans l'utilisation de la reconnaissance faciale c'est le respect du principe de finalité. Les données personnelles récoltées doivent avoir un but précis, un délai de conservation défini et une notification doit être émise au moment de leur collecte. Ce principe de finalité est complémenté par un principe de proportionnalité que la jurisprudence a développé pour assurer une meilleure protection des données personnelles.

3.1. Le principe de proportionnalité, garde-fou des données personnelles.

On constate de nos jours une banalisation de la reconnaissance faciale, des millions de personnes déverrouillent leurs smartphones grâce au logiciel de *FaceID* de la compagnie Apple, tandis que d'autres utilisent les services de reconnaissance faciale de Facebook pour identifier leurs amis sur les photos. Toutes ces utilisations ne sont pas sans conséquence pour la vie privée, puisque chaque photo est enregistrée dans une base de données. Ces entreprises-là peuvent par la suite utiliser ces images à d'autres fins comme le suivi du comportement ou des fins commerciales.

Avec la refonte de la Loi Informatique et Liberté en 2004, la CNIL avait le droit d'autoriser les dispositifs biométriques privés et elle pouvait émettre un avis sur l'utilisation faite par l'Etat. Les utilisations de la biométrie se sont très vite multipliées comme le démontre le tableau suivant. En effet, la CNIL a traité 45 demandes en 2005 et 465 demandes en 2007, ce chiffre n'a cessé d'augmenter depuis. Rappelons néanmoins que depuis l'adoption du RGPD, il n'est plus obligatoire pour les entreprises de saisir la CNIL pour les demandes de traitement des données personnelles.

Statistiques sur les demandes d'autorisation présentées à la CNIL de 2004 au 10 mars 2014

	Demandes d'autorisation		Autorisations délivrées			Refus
Année	Nb de demandes entrant dans le champ d'une autorisation unique	**Nb total de demandes**	Nb d'autorisations « spécifiques »	Nb d'autorisations *via* un engagement de conformité à une AU	**Nb total d'autorisations délivrées**	**Nb de refus**
2004	1	**1**	0	1	**1**	**0**
2005	8	**45**	30	8	**38**	**5**
2006	258	**326**	59	258	**317**	**9**
2007	399	**465**	45	399	**444**	**21**
2008	550	**630**	61	550	**611**	**19**
2009	676	**747**	68	676	**744**	**3**
2010	555	**581**	22	555	**577**	**4**
2011	595	**631**	28	595	**623**	**8**
2012	626	**648**	22	626	**648**	**0**
2013	357	**385**	5	357	**362**	**12**
2014	13	**22**	0	13	**13**	**0**
TOTAL	4038	**4481**	340	4038	**4378**	**81[1]**

Source : commission des lois à partir des données fournies par la CNIL

Figure 3: Statistique sur les demandes d'autorisation présentées à la CNIL entre 2004 et mars 2014. Source : CNIL

Très tôt la jurisprudence, plus particulièrement la CEDH, a réagi pour garantir une protection aux individus[28] en consacrant le principe de proportionnalité pour l'utilisation des données biométriques. Ce principe implique que le traitement des données à caractères personnelles doit se faire pour des finalités déterminées, explicites et légitimes. Elles doivent également être conservées pendant une durée qui n'excède pas celle qui est nécessaire aux finalités pour lesquelles elles sont traitées et collectées. Néanmoins ce principe de proportionnalité a été interprété de manière différente entre les États membres de l'Union européenne. Comme le souligne le rapport de l'ENISA de 2009, aucun Etat n'applique les mêmes exigences en matière de biométrie et de la protection des données biométriques. Il convient également de préciser que la CJUE aussi prône une vision différente de la CEDH, puisqu'elle

[28] CEDH, S. et Marper c. Royaume-Uni, 2008 + CEDH, 18 avril. 2013, M.K. c. France, n° 19522/09

autorise l'utilisation par les autorités des données biométriques du passeport à toutes les fins[29].

Ainsi, en France le partage de données biométrique est interdit tandis qu'au Royaume-Uni il est autorisé notamment depuis le *Serious Crime Act* de 2007. L'autre exemple d'interprétation différente se trouve dans la durée de conservation des données, les divergences persistent également sur ce sujet puisque l'Allemagne conserve les données pour 10 ans maximum, le Royaume Uni, jusqu'à l'arrêt S. et Marper, conservait les données indéfiniment et la France applique une conservation graduelle en fonction de catégorie de la personne concernée : 40 ans si elle a été condamnée, 25 ans si elle a été mise en cause lors d'une procédure pénale[30].

Au niveau national, en France, la loi informatique et liberté de 1978 prévoit une limite sur le caractère de la donnée biométrique à traiter et instaure dès le début une proportionnalité dans le traitement de ces données. Le Conseil d'Etat a reconnu le principe de proportionnalité pour le traitement des données personnelles dans une décision rendue en Assemblée plénière le 26 octobre 2011 (n°317827) : « *Considérant qu'il résulte de l'ensemble de ces dispositions que l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités*. »

La biométrie faciale étant une donnée personnelle, elle rentre dans le champ d'application de cette décision rendue par le Conseil d'Etat.

3.2. L'expansion du principe de proportionnalité à l'ensemble du processus de traitement.

Ce principe de proportionnalité doit aller au-delà du simple prélèvement de la donnée biométrique et s'appliquer au traitement des personnes qui ont été reconnues par la caméra. Pour mieux comprendre cet argument nous proposons l'analogie

[29] CJUE, 4e ch., 16 avril 2015, W. P. Willems e.a. c. Burgemeester van Nuth e.a et CJUE Affaire Schwarz du 17 octobre 2013.
[30] Article R.53-14 du Code de procédure pénale

suivante : Dans les aéroports lorsqu'un voyageur passe les postes d'inspection filtrage (PIF) et que le détecteur de métal sonne, la palpation est une réponse proportionnelle. Lorsque la caméra reconnait un individu comme étant « recherché », il faut continuer à appliquer la présomption d'innocence et ne pas le traiter comme s'il était coupable. Cette situation a été vécue à l'aéroport international de Fresno Yosemite aux Etats-Unis qui avait installé un système de reconnaissance faciale. Un passager a déclenché une alarme en passant devant la caméra et les agents du FBI ont interpellé l'individu et l'ont retenu en garde à vue pour la nuit[31].

La proportionnalité du traitement des données personnelles et biométrique s'applique également à la structure de conservation desdits données. En effet, la CNIL[32] et le G29[33] sont fermement opposés à la mise en place d'une base de données centralisée sauf si un impératif de sécurité l'exige. Plus tard, le Conseil Constitutionnel dans une décision du 22 mars 2012 (N°2012-265 DC), censurant la loi du 2012 sur la protection de l'identité, va aussi interdire la généralisation d'une base centralisée à l'ensemble des données collectées au titre des documents d'identité et la possibilité de consulter le fichier à des fins d'identification à partir des seules données biométriques. L'utilisation d'un support contenant les informations biométriques en possession de l'individu est souvent privilégiée car il offre une meilleure protection des données contre l'utilisation frauduleuse.

Le CEPD s'est également opposé contre l'interopérabilité des données présentes dans une base de données. En effet, le 10 mars 2006, il a émis un avis à la Commission européenne qui considérait l'interopérabilité comme un concept technique plutôt que juridique. Le contrôleur européen estime que « *rendre techniquement possible l'accès à des données ou leur échange constitue dans de nombreux cas une puissante incitation à y accéder de facto ou les échanger* ». En effet, chaque entreprise biométrique a sa manière de traiter la donnée mais leur distinction repose sur des points mineurs et ceci rend possible l'interopérabilité des données. Le danger de la biométrie et de la reconnaissance faciale c'est la généralisation de l'interconnexions

[31] L. D. Introna et H. Nissenbaum, Facial Recognition Technology : a survey of policity and implementation issues, p.45

[32] Délibération n°2007-368 du 11/12/2007 de la CNIL par rapport au passeport biométrique : L'utilisation d'une base de donnée centralisée pour le traitement des données de biométrie à trace pose problème.

[33] Avis 3/2005

des fichiers pouvant favoriser la mise en place d'un « *Big Brother* » administratif en traçant les individus comme c'est le cas actuellement en Chine.

3.3. L'effacement de l'obligation de consentement au profit du devoir d'information

Avec la diffusion globale des technologies biométriques, on constate que le principe de consentement s'efface au profit du devoir d'information. L'article 7 de la loi informatique et liberté du 6 janvier 1978 indique que « *un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée* » mais précise immédiatement après que le consentement n'est pas nécessaire dans certaines hypothèses, telles que « *le respect d'une obligation légale incombant au responsable du traitement* », « *la sauvegarde de la vie de la personne concernée* » ou encore « *la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée ».* Compte tenu de l'utilisation massive de la biométrie faciale, il serait de nos jours très difficile de recueillir le consentement de tout individu pour chaque traitement de leurs données personnelles.

Pour résoudre ce problème, le Règlement général sur la protection des données applicable impose une obligation d'information qui doit être concise, transparent compréhensible et aisément accessible des personnes concernées. Ces obligations sont définies aux articles suivant :

- Article 12 intitulé « *Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée* »,
- Article 13 intitulé « *Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée* »,
- Article 14 du règlement « *Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée* ».

On retrouve cette obligation d'information dans les autres textes visant à protéger la vie privée, comme le BIPA adopté en 2008 par l'Illinois ou le SB 169 adopté en 2001 par la Californie.

3.4. Le respect de la vie privée comme vecteur d'innovation.

Afin d'assurer le respect de la vie privée, il est possible de recourir à la biométrie dite non-traçable. Le terme de biométrie non-traçable regroupe trois types de technologies de *Privacy by design* : le cryptage biométrique, la biométrie révocable et la biométrie anonyme (ou biométrie « désidentifiée »). Leur objectif est de transformer de manière irréversible les données biométriques de la personne afin qu'elle ne puisse pas être identifiée[34]. À ce sujet, le G29 a émis une recommandation le 22 mars 2012 (Avis 02/2012, N°00727/12/FR WP192) sur la reconnaissance faciale dans le cadre des services en ligne et mobile. En outre il fait référence au cryptage biométrique et à la biométrie non traçable comme solution permettant de protéger la vie privée des personnes. Il fait également référence au cryptage biométrique dans sa recommandation du 27 avril 2012 sur l'évolution des technologies biométriques.

Citées précédemment, les institutions européennes comme le CEPD, la CJUE ou encore le CEDH n'hésitent pas à se mobiliser pour montrer leur opposition contre des accords passés par les Etats. Le CEPD a réussi notamment à imposer ses motivations dans des dossiers sensibles comme l'accord « *Passenger Name Record* » conclu entre l'Union européenne et les Etats-Unis.La CJUE avait également annulé le premier accord entre les Etats-Unis et l'Union européenne pour des raisons de procédure. Quant à la CEDH, elle conserve sa position protectrice en s'appuyant surtout sur l'article 8 de la Convention européenne des droits de l'homme (Conv. EDH).

Compte tenu du rôle central des aéroports dans les attentats « fondateurs » de la biométrie, les technique d'identification ont pris une place essentielle en terme de renforcement de la sécurité aérienne, mais aussi en terme de rapidité de traitement du flux des passagers. De ce fait, notre réflexion sera axée principalement sur l'utilisation de la reconnaissance faciale au sein des aéroports. Ainsi, l'analyse de l'utilisation faite par les autorités notamment dans le cadre de la recherche de criminels et des contrôles aux frontières (**Partie 1**) précédera l'étude de l'utilisation faite par les gestionnaires aéroportuaires tant pour améliorer l'expérience du passager que pour contrôler les accès en ZSAR (**Partie 2**).

[34] https://www.biometrie-online.net/biometrie/biometrie-et-vie-privee

Partie 1 :
L'utilisation de la reconnaissance faciale par les autorités : recherche de criminels et contrôle aux frontières.

Il n'y a pas de doutes, les personnes publiques sont les moteurs de l'industrie biométrique. Elles utilisent la reconnaissance faciale principalement pour deux cas de figure : retrouver des criminels et contrôler l'accès sur leur territoire. Néanmoins, ces deux approches sont différentes l'une de l'autre dans la mesure où la première se fait en *open-set* alors que la seconde sera en *closed-set*[35].

D'autres caractéristiques que l'on développera dans cette partie distinguent ces utilisations, mais la réalité nous oblige à admettre que le premier cas de figure reste très difficile à mettre en place notamment dans les sociétés démocratiques tandis que le second se trouve déjà présent sur plusieurs aéroports à travers le monde.

Très souvent le déploiement des systèmes de biométrie faciale n'est pas là pour servir les personnes qui s'y soumettent, au contraire ils s'imposent aux personnes désireuses d'exercer un droit ou de bénéficier d'un service (*i.e.* liberté de mouvement, demande d'asile).

Par conséquent, l'analyse des faiblesses de l'utilisation de la reconnaissance faciale dans la recherche de criminel (**Titre 1**) précèdera l'étude de l'utilisation de la reconnaissance faciale pour renforcer le contrôle au frontière (**Titre 2**).

[35] On parle d'*open-set* lorsque la reconnaissance faciale agit dans un environnement non contrôlé et qu'il n'y a pas de certitude sur l'enrôlement des personnes recherché dans la base de donnée (espace public). Le *closed-set* quant à lui est la situation dans laquelle nous savons que les personnes sont enrôlées dans la base de données (accès en zone restreint).

Titre 1 :
Les faiblesses de la reconnaissance faciale dans la recherche des criminels.

La recherche de criminels avec la reconnaissance faciale s'inscrit dans ce que l'on appelle en anglais le « *policing* ». Il s'agit en outre de l'art d'assurer des missions de lutte contre le crime ou des déviances et pour le maintien de l'ordre indépendamment de l'agent dédié à cet office. Assurer la sécurité de ses citoyens et empêcher tout trouble à l'ordre public sont les motivations principales des autorités publiques qui les poussent à investir dans la reconnaissance faciale.

Néanmoins, cette volonté de la part des autorités fait face à différents types d'obstacles. Les systèmes de reconnaissance faciale ont été pendant longtemps lacunaires en terme de performance, mais aujourd'hui l'obstacle majeur est lié à l'acceptation par l'opinion publique de cette technologie. On remarque alors que le déploiement en masse de la biométrie faciale doit faire face à aux difficultés techniques inhérentes aux avancées technologiques (**Chapitre 1**) et surmonter les obstacles sociétaux qui se manifestent notamment dans les pays démocratiques (**Chapitre 2**).

Chapitre 1 :
L'évolution des difficultés techniques de la reconnaissance faciale

La reconnaissance faciale a eu des débuts difficiles à cause d'un déploiement précipité. Les ambitions étaient fortes aux lendemains des attentats du 11 septembre 2001, mais les techniques n'étaient pas encore au point pour en faire un usage dans les milieux publics. Avec des échecs à répétition dans différents domaines (I), la reconnaissance faciale a nécessité des améliorations (II).

I. Des échecs à répétition de la reconnaissance faciale.

La reconnaissance faciale est une technologie complexe et hybride, elle marque une rupture avec les techniques d'identification traditionnelle en combinant plusieurs finalités (identification, surveillance, lutte contre le terrorisme). Sa multi-finalité empêche de l'appréhender comme une NTIC classique[36] et bien que plusieurs tests ait été menés pour l'identification de criminel, ces tests n'ont pas eu de suite opérationnelle.

1.1. Des expériences infructueuses au niveau mondial

La première expérience biométrique a été réalisée à Amsterdam avec le « *Schiphol Pass Travel* » en 1992. Cet outil biométrique reposant sur l'empreinte digitale a été très vite abandonné car le public s'est rendu compte qu'il était possible de contourner le système avec des faux doigts en silicone. Quant à l'utilisation de la reconnaissance faciale pour la recherche de criminel elle a d'abord eu lieu dans une ville de Floride aux Etats-Unis en 2001[37]. La ville de Tampa avait passé un contrat avec la société *Visionics* pour déployer la technologie dans ses rues mais aussi pour l'évènement sportif de l'année, le *Super Bowl*, qui s'est tenu dans la ville. Pendant la finale, 100 000 fans ont été analysés par la caméra et leur image a été comparée à une base de données de 1 700 criminels. Il y eu au total 19 « *hit* », mais uniquement un seul a nécessité l'intervention de la police.

[36] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 20, *« Acceptabilité » de la biométrie : linéaments d'un cadre analytique,* §40

[37] D. McCormack, *« Can Corporate America secure our nation ? An analysis of the Identix Framework for the regulation and use of facial recognition technology »,* p.6

L'expérience a été très courte puisque seulement six mois après son déploiement, les autorités de police avaient abandonné l'utilisation de la technologie et l'opposition au sein de l'opinion publique augmentait. A l'instar de Tampa, la ville de Virginia Beach dans l'Etat du Virginia et la ville d'Oakland en Californie ont également voulu déployer cette technologie. Bien que la première ait réussi à faire passer la motion d'adoption, la deuxième n'a pas récolté le vote nécessaire pour l'utilisation de cette technologie aux fins de police.

Toujours aux Etats-Unis, c'est l'aéroport de Logan à Boston qui va lancer l'utilisation de la reconnaissance faciale avec les entreprise *Viisage* et *Identix* en mai 2002. Bien que les défauts étaient visibles, les deux sociétés indiquaient que leur technologie avec un taux de réussite de 90%. Les résultats en laboratoires ne sont pas pertinents lorsqu'il faut déployer la technologie à grande échelle car la réalité du terrain présente davantage de complexité que l'on ne peut pas envisager en laboratoire et c'est pour cela que les entreprises n'ont pas été capable de surmonter les problèmes techniques. Lorsque la caméra était réglée en mode sensible, beaucoup de personnes obtenaient des rapprochements avec les individus recherchés. Et vice-versa, lorsqu'elle était réglée à un niveau plus robuste, aucune personne n'était reconnue[38]. Souvent les coûts financiers conduisent également à abandonner les systèmes de reconnaissance faciale.

1.2. La difficulté dans l'utilisation des caméras de surveillance pour la reconnaissance faciale.

Il est également possible d'utiliser la reconnaissance faciale à l'aide des caméras de surveillance, mais cette technique pose un problème d'installation. Les caméras de surveillance sont souvent placées en hauteur et l'angle de la caméra ne permet pas d'identifier les visages. En Allemagne, l'Office fédérale de police criminelle (*Bundeskriminalamt – BKA)* a publié un rapport sur la reconnaissance faciale suite à un test qu'ils avaient effectué dans la gare de la ville du Mainz[39]. D'octobre 2006 à janvier 2007 une caméra de surveillance a été placée pour identifier le visage des suspects avec un paramétrage FAR à 1%.

[38] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* – Chapitre 7 *: le taux d'erreur dans le recours aux identifiant biométriques* par B. Dorizzi, §35

[39] L. D. Introna et H. Nissenbaum, *Facial Recognition Technology : a survey of policity and implementation issues*, p.39

Selon le rapport, la reconnaissance faciale n'atteint pas les niveaux requis pour un déploiement en masse puisqu'en journée, le taux de reconnaissance était de 60% et ce chiffre diminuait une fois la nuit tombée. Par ailleurs le rapport constate également que la qualité de la caméra influe considérablement sur les résultats de la reconnaissance faciale. Enfin ce rapport conclu en indiquant que la reconnaissance faciale doit être utilisée dans un environnement fermé, où les variations dans l'illumination restent très faibles voire inexistantes afin de fonctionner correctement.

Plus récemment, au début de l'année 2019, la ville de Nice a fait une expérimentation de la reconnaissance faciale lors du carnaval. Le test qui a duré deux jours avec 1000 volontaires devait permettre de simuler des situations différentes : retrouver des enfants perdus, localiser les personnes âgées vulnérables ou encore retrouver les personnes d'intérêts (recherchées). Depuis l'entrée en vigueur du RGPD, la CNIL n'a plus l'obligation de donner une autorisation préalable pour les équipements biométriques, mais si l'on analyse ses précédentes décisions on peut penser que son contrôle *a posteriori* conduira probablement à l'annulation de cette procédure. En effet, lors d'un communiqué[40] sur le sujet elle a clairement indiqué que ce genre de pratique ne peut passer au-delà du test car aucune loi n'encadre l'utilisation de la reconnaissance faciale dans le domaine public en France.

1.3. Une possibilité d'aller au-delà de la simple identification.

A côté de la reconnaissance faciale se développe également une technologie similaire mais plus ambitieuse : l'analyse automatique des expressions du visage ou encore l'AFEA[41]. Cette technologie se rapproche de ce qu'on appelle la biométrie comportementale.

L'AFEA permet d'aller plus loin que la simple reconnaissance d'identité ou l'authentification car elle permet d'anticiper les comportements des individus grâce aux expressions de leur visage. Cela étant, les travaux sur cette technologie sont encore en phase de recherche et très peu d'expérimentation opérationnelle de « masse » ont été réalisées.

[40] https://www.nextinpact.com/news/107628-reconnaissance-faciale-ville-nice-na-pas-recu-dautorisationde-cnil.htm
[41] K.A. Gates, *Our Biometric Future : Facial Recognition Technology and the culture of surveillance*, p.8

II. Les améliorations nécessaires pour la reconnaissance faciale.

Pour que cette technologie puisse fonctionner il faut pouvoir établir une base de données où sont enrôlés les criminels. Bien que le prélèvement d'empreinte biométrique nécessite un consentement, en matière pénal les pratiques sont un peu plus compliquées. Ainsi, quel que soit le degré d'implication de la personne dans la commission d'une infraction, on peut le contraindre à donner son empreinte digitale ou son image car le refus de se prêter à un prélèvement corporel est aussi sanctionné par la loi[42].

2.1. La nécessité d'établir une de base de données cohérente

La création de la base de données pour la recherche de criminel n'est pas très difficile puisque les données biométriques des criminels peuvent être récoltées plus aisément. Il faut par ailleurs définir un équilibre entre sécurité nationale et ordre public en déterminant quel type de personne recherche-t-on aux seins de aéroports. On peut par exemple cibler la recherche sur des terroristes, des agresseurs sexuels ou des enfants perdus. Le principe de proportionnalité exige un délai limité dans la conservation des données, ainsi les juges et les autorités pourront décider conjointement si une personne peut être retirée de la base de données lorsqu'elle ne pose plus de menaces. Toutefois, il faut rappeler que la caméra enregistre le visage de toutes les personnes qui passent devant elle. Afin de lutter contre la création d'une base de donnée des personnes innocentes, il faudrait que le logiciel soit équipé d'un système qui n'enregistre pas l'image tant qu'elle n'a pas établi de correspondance avec une image présente sa base de données.[43]

Pour inciter à la biométrie et à l'utilisation de la reconnaissance faciale, le FBI a annoncé deux initiatives en 2008. La première c'est la *Next generation identification* qui a pour but d'instaurer un fichier mondial sur les données corporelles aux Etats-Unis à des fins policières. Les employeurs pourront éventuellement accéder à ce fichier afin de connaître la provenance de leurs employés. L'autre initiative est intitulée « *Server in the sky* », elle prendra la forme d'une base de données

[42] Article 706-56 du Code de procédure pénale, alinéa 3.
[43] D. McCormack, *« Can Corporate America secure our nation ? An analysis of the Identix Framework for the regulation and use of facial recognition technology », p.25*

internationale permettant au FBI de collaborer avec d'autres institutions notamment des pays comme le Canada, le Royaume-Uni et l'Australie[44] pour la recherche de criminel.

Les bases de données utilisées doivent être également sécurisées dans la mesure où ces dernières ne sont pas à l'abris de cyber attaques. En Mai 2019, le CBP a appris que les données des plaques d'immatriculation ainsi que les photos de 100 000 personnes ont été fuitées par un sous-traitant du gouvernement[45].

2.2. La réduction du FAR pour l'extension de l'utilisation de la reconnaissance faciale

L'amélioration la plus importante réside dans la réduction du FAR. En effet, les fausses acceptations pourront donner à une personne non autorisée l'accès à des zones sensibles. Pour les zones stratégiques et très fréquentées, le taux de fausse acceptation doit être de 1/100 000 afin d'assurer une sécurité optimale et un confort aux usagers. Les différentes technologies ont en moyenne des FAR de l'ordre suivant :

- Empreinte digitale de 0,005% à 0,1%
- L'iris 0.0001%
- La main 0,1%.
- Le visage 0.3% à 5%.

En dessous de ce chiffre, les résultats conduiront à une dégradation de l'utilité de la technologie. Par exemple, si on met en place un système de reconnaissance faciale efficace à 99.99%. Avec un FAR de 1/10 000. Dans le cas d'un aéroport qui traite 10 millions de passagers par an cela reviendrait à 1000 erreurs dans la recherche de suspect et parmi ces 1000 erreur, seul une personne sera en effet recherchée. Ce FAR va nuire à la sécurité dans le sens où les efforts consacrés aux fausses alarmes auraient pu être affectés ailleurs. D'autres part, les agents de sécurité risque d'avoir un comportement de moins en moins attentifs face aux alarmes.

[44] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 18 par D. Lyon, *Les insignes corporelles : la biométrie comme perte de l'histoire personnelle*, §1 et §2
[45] https://techcrunch.com/2019/06/10/cbp-data-breach/

Néanmoins, ces obstacles techniques semblent aujourd'hui surmontés puisque durant les FRVT effectués par le NIST, la caméra de la compagnie GE Global Research a pu notamment suivre un individu depuis 25-50 mètres et le reconnaître d'une distance de 15-20 mètres avec une base de données de 1.6 millions d'images. La détection de visage dans la foule dépend principalement des variations dans l'éclairage des visages et de leur orientation.

La technologie a également connu une révolution en 2016-2017 en basculant sur les réseaux de neurones. Par exemple, la solution Gemalto peut détecter plus de 100 visages par image dans une foule et la limitation provient seulement des moyens matériels (serveur, cartes graphiques, caméras). Puisqu'il faut une certaine qualité d'image pour bien reconnaître la personne, il vaut mieux filmer les individus en amont que d'attendre qu'il se rassemble. Force est de constater qu'aujourd'hui le problème principal de la reconnaissance faciale réside dans son acceptation par la société.

Chapitre 2 :
Le développement des obstacles sociétaux face à la reconnaissance faciale

La reconnaissance faciale permet de filtrer les individus en déterminant s'ils font partie d'une liste de suspect ou non. Face à un risque terroriste angoissant dont les probabilités sont faibles mais les conséquences dramatiques, les autorités favorisent l'option à zéro risque en éliminant la menace au lieu de la gérer. Mais cette pratique conduit à un déséquilibre d'informations qui fait régner un sentiment de discrimination (I) et se heurte à des oppositions marquantes au sein de la société (II).

I. Un déséquilibre d'information à l'origine du sentiment de discrimination.

Certes, nous sommes loin du modèle « orwellien » mais les avancées en terme de technologie sont rapides et performantes, ce qui nous rapproche de ce scénario. À titre d'exemple, les autorités chinoises ont développé un système de reconnaissance faciale qui permet d'identifier un visage dans une foule de 50 000 personnes.

En outre, la Chine utilise cette technologie à d'autres finalités aussi, notamment en donnant des « notes » de bonne conduite à chaque citoyen, sachant que plus la note est bonne plus on a des privilèges, plus elle est mauvaise plus on a des restrictions. On peut comparer cette pratique à l'attribution d'un « crédit social » aux citoyens.

1.1. Un manque de visibilité dans le traitement des données faciale

Cet exemple chinois reste unique dans le monde, d'autant plus qu'il est pratiqué dans un pays où les technologies sont à la pointe et le gouvernement autoritaire en profite pour ses intérêts. Dans les pays occidentaux, il est plus difficile de créer une base de données pour les administrés car le prélèvement de données personnelles à de telle fin a toujours eu une connotation négative puisqu'elle est assimilée à la criminalité.

Il existe également un déficit d'information sur la technologie biométrique, les citoyens ne sont pas ou peu intéressé sur l'impact que peut avoir la reconnaissance

faciale sur leur quotidien. Comme le souligne Kelly A. Gates dans son ouvrage[46], on remarque dans les sociétés occidentales un paradoxe entre le libre choix et la gouvernance disciplinaire dans la mesure où le marché est très souvent libre mais ce dernier surveille beaucoup les comportements des individus et ce grâce aux données personnelles récoltées.

Le déséquilibre provient du fait que les utilisateurs de la reconnaissance faciale sont souvent anonymes et non vus ce qui crée des suspicions de plus en plus forte. Cela se rapproche de la métaphore panoptique développée par Michel Foucault où les détenus d'une prison sont surveillés à tout moment par le gardien sans que ce dernier soit visible par eux. Se pose la question alors de savoir si la capacité de reconnaître une personne discrètement et de loin est acceptable dans les sociétés libres où le consentement et la présomption d'innocence règne. Les jurisprudences sur le respect de la finalité et le contrôle de la proportionnalité interviennent comme protecteur des citoyens et de leur vie privée

On remarque également que pour les documents de voyage, les individus sont contraints de révéler davantage d'informations, tandis que les pouvoirs publics sont de plus en plus discrets et opaques par rapport au développement des nouvelles méthodes d'identification. Cela s'explique souvent par la complexité technique des nouvelles technologies mais aussi dans un souci de protéger les organisations étatiques des regards et de la responsabilité[47].

1.2. Le respect de la finalité principale de la reconnaissance faciale

Le but dans l'utilisation de la reconnaissance faciale ne doit pas être de déterminer l'origine ethnique de la personne mais uniquement d'identifier les visages. Toutefois, il s'avère que la technologie est discriminante envers les personnes de couleurs, ce qui est contraire au principe des sociétés qui prônent l'égalité. La biométrie confirme et renforce le caractère sélectif : les Noirs sont plus « biométrisés » que les Blancs dans certains États des États-Unis.

[46] K. A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance (Critical Cultural Communication,* p.196

[47] B. McPhail, C. Parsons, K.L Smith, J. Ferenbok & A.Clement, *Identifying Canadians at the Border : ePassports and the 9/11 legacy*, p.355 : le terme utilisé est *accountability* qui correspond plus à l'imputabilité que la responsabilité juridiquement parlant.

Ce fut le cas à San Francisco notamment où le système de reconnaissance faciale avait tendance à identifier davantage les personnes de couleurs comme faisant partie d'une liste de suspect[48], c'est pour cela qu'elle a été abandonnée par la ville. Selon de Kelly A. Gates « *Les sociétés les plus pacifiques ne sont pas celles où il y a de la surveillance partout mais les sociétés où les différences culturelles sont respectées et les gens ont un contrôle sur leur vie* ». Une autre approche tend à dire que la généralisation de cette technologie et le caractère automatisé de la lecture des données pourraient aussi faire voler en éclats l'arrière-plan discriminatoire dont elle hérite.

En dépit des limites posées par le principe de finalité, on est loin d'une protection maximale. Selon le CEPD[49], dans le cadre des transferts de données à but répressif, aucune garantie juridique ne permet de toute évidence d'être assurée de la finalité précise pour laquelle les données seront utilisées une fois transférées.

II. Les oppositions marquantes au sein de la société.

Attaché l'identité au corps à travers la biométrie est perçu comme un élément clé de la gouvernance des populations dans l'ordre socio-politique tant au niveau national qu'international[50]. Plus la population augmente, plus il devient difficile de la « contrôler » et l'utilisation des technologies de pointe devient la solution que choisisse les autorités.

2.1. Des mouvements civils jusqu'à l'interdiction de la reconnaissance faciale

Face à ces utilisations massives de la part des pouvoirs publics, un mécontentement au sein de l'opinion publique se manifeste. Les individus se mobilisent contre l'utilisation de la reconnaissance faciale et leurs manifestations réussies à aboutir.

En 2007, les locaux de la CNIL ont été occupés par des militants de différentes organisations contre la biométrie comme Oblomoff, Pièces et Main D'Oeuvre, du

[48] T. Lozier (Security Magazine), *In the Age of facial recognition, the Human element is still necessary*, date de publication : 29/05/2019

[49] Troisième avis du CEPD sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale » (J.O. C.E 139, 23 juin 2007)

[50] D. Introna et H. Nissenbaum, *Facial Recognition Technology : a survey of policity and implementation issues*, p.10

Mouvement pour l'Abolition de la Carte d'Identité (MACI), de « Halte aux puces ! », « Coordination contre la biométrie », et « Souriez, vous êtes filmés ! ». Ils ont débattu avec les employés et ont dissous la CNIL car ils estiment que celle-ci n'a plus d'indépendance concrète vis-à-vis de l'Etat. Leurs slogans étaient assez marquants, ils affichent entre autres les expressions suivantes : « *Informatique ou liberté, il faut choisir* » ou « *L'Etat contrôle la CNIL* ».

Au Royaume-Uni, l'association Big Brother Watch dénonce l'inefficacité et l'incohérence de l'utilisation de la reconnaissance faciale qui n'est fiable. Elle a publié sur son site internet les chiffres de la police britannique concernant les résultats de

LIST OF EVENTS AND DATES WHERE SOUTH WALES POLICE HAS USED AFR

Show 10 entries Search:

Event	Date	True-positives	False-positives	Police wrongly stopping innocent people ('interventions')
UEFA Champions League Final Week (Cardiff Airport, Train station and City Centre)	29/05/2017 - 03/06/2017	173	2,554	5
Elvis Festival (Porthcawl)	23/09/2017 - 24/09/2017	10	7	1
Operation Fulcrum 'Day of Action' (Cardiff)	19/10/2017	5	11	2
Anthony Joshua v Kubrat Pulev Boxing (Cardiff)	28/10/2017	5	46	2
Wales v Australia Rugby (Cardiff)	11/11/2017	6	42	2
Wales v Georgia Rugby (Cardiff)	18/11/2017	1	2	0
Wales v New Zealand Rugby (Cardiff)	25/11/2017	3	9	2
Wales v South Africa Rugby (Cardiff)	02/12/2017	5	18	5
Kasabian Concert (Motorpoint Arena, Cardiff)	04/12/2017	4	3	0
Liam Gallagher Concert (Motorpoint Arena, Cardiff)	13/12/2017	6	0	0

Showing 1 to 10 of 43 entries Previous Next

Figure 4: Tableau montrant les évènements pour lesquels la police britannique a utilisé la reconnaissance faciale avec le nombre de correspondance réussie (True positive), le nombre de fausse acceptation et le nombre d'interventions de la police conduisant à l'arrestation de personnes innocente.
Source : https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/

l'utilisation de la reconnaissance faciale (figure 3).

D'autre part, en mai 2019 la ville de San Francisco a interdit l'utilisation de la reconnaissance faciale par la police dans la recherche de criminels. Néanmoins, la ville continue d'utiliser la technologie pour l'aéroport, le port maritime et autorise les personnes privées à en faire usage.

2.2. Les limitations imposées par les autorités de protection des données et les juges.

La CNIL a comme mission principal la protection du respect au droit à la vie privée[51]. De ce fait, elle avait tendance à autoriser systématiquement l'utilisation des outils biométriques ne nécessitant pas de base de données centralisée, la CNIL autorise systématiquement le système. Mais lorsque les données biométriques de référence sont enregistrées dans un système centralisé, elle effectuait un strict contrôle de la finalité et autorise le système uniquement lorsqu'il y a un impératif de sécurité. Avec l'entrée en vigueur du RGPD, le contrôle *a priori* de la CNIL a été supprimé, ce qui réduit ainsi son rôle car il n'y a plus d'obligation de déclaration à faire auprès de celle-ci pour effectuer un traitement de données personnelles et biométriques. Cela étant les sanctions prévues par le RGPD sont très lourdes et dissuasives pour les utilisations abusives.

Les juges européens et nationaux sont également protecteurs du droit au respect de la vie privée notamment avec le principe de proportionnalité qui empêche l'utilisation abusive de la reconnaissance faciale. D'autre part, les sénateurs avaient soumis une proposition au Sénat pour limiter l'utilisation de la biométrie[52]. Suite au 11 septembre 2001, les sociétés occidentales ont favorisé les solutions high-tech, peut-être parce qu'on trouve une dimension spectaculaire dans l'utilisation de ces technologies pour contrecarrer un risque lui-même spectaculaire[53].

Aux Etats-Unis, le Comité d'observation des droits et libertés civiles (PCLOB) a annoncé qu'il allait examiné l'utilisation faite de la reconnaissance faciale dans les aéroports américains[54].

La reconnaissance d'un visage dans une foule est comparable à un « Grand prix de l'identification ». Aujourd'hui, bien que des difficultés persistent, le challenge semble avoir été relevé par les entreprises du secteur. Tant dans l'avancée de la technologie que dans les pratiques, la reconnaissance faciale est devenue une méthode

[51] https://www.cnil.fr/fr/les-missions-de-la-cnil
[52] http://www.senat.fr/rap/l13-465/l13-465_mono.html
[53] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 18 par D. Lyon, *Les insignes corporelles : la biométrie comme perte de l'histoire personnelle,* §26
[54] https://thehill.com/policy/technology/450930-government-privacy-watchdog-to-probe-use-of-facial-recognition-tech-at

incontournable d'identification. Elle est la méthode de biométrie privilégiée par les autorités pour le contrôle des frontières.

Les sas présents dans les aéroports permettent de pallier les difficultés de la reconnaissance faciale que l'on rencontre dans un espace public puisque les personnes sont confinées dans un milieu contrôlé et passe un par un devant la caméra. Les dangers liés à son utilisation dans les espaces publics ne sont pas retrouvables lors des « *due process*[55] » (procédure régulière) puisqu'une meilleure protection des données et de la vie privée est assurée lorsqu'il s'agit de contrôler les passages aux frontières. Tout un encadrement est mis en place pour éviter les dérives tant par les agents de police que par les utilisateurs.

[55] P.E. Agre, *Your face is not a bar code,* 10.09.2003 : https://pages.gseis.ucla.edu/faculty/agre/bar-code.html :

Titre 2 :
Le renforcement du contrôle aux frontières avec la reconnaissance faciale.

La reconnaissance faciale est aujourd'hui utilisée par les autorités étatiques surtout pour les contrôles aux frontières. L'augmentation continue du nombre de voyageurs, 4 milliards de passager en 2017 selon IATA, augmente aussi *de facto* les risques de fraude documentaire nécessitant l'adoption de solution technologiques plus efficace.

En 2013, environ 7 millions de cartes nationales d'identité et 3,8 millions de passeports ont été produits. Les experts estiment que le taux de fraudes se situe dans une fourchette qui va de 3 à 6% selon le type de titre produit. En fonction des coûts de production des titres, le prix de la fraude représente directement 1 à 2 millions d'euros, sachant que ceci est inférieure aux conséquences de l'utilisation de tels documents.

Bien que la reconnaissance faciale ait eu des débuts précaires (**Chapitre 1**), elle est aujourd'hui un outil utilisé mondialement (**Chapitre 2**).

Chapitre 1 :
Les débuts précaires de la reconnaissance faciale pour le contrôle aux frontières

Le visage a été rapidement choisi comme élément clé de l'identification d'une personne par l'OACI et ses Etats membres (I). Néanmoins, le manque de standard technologique entre les pays (II) était un obstacle non négligeable pour l'optimisation de la reconnaissance faciale.

I. Le visage en tant qu'identifiant de la personne.

1.1. Le corps ne ment jamais

La peur de ne pas être en mesure de contrôler tous les risques qui découle pour la sécurité et la souveraineté a poussé les Etats à prendre des dispositions pour renforcer la sécurité de leur frontière. Il leur fallait donc à tout prix identifier avec certitude qui est qui en assignant une identité fixe, inaltérable et universellement reconnaissable. De manière générale, l'utilisation du corps comme identifiant découle de l'idée selon laquelle « *le corps ne ment jamais* »[56]. Or, comme il a été vu dans des exemples précités jusqu'à présent, les tentatives de fraudes biométriques existent et certains aboutissent plus facilement que d'autre.

L'outil idéal pour diffuser l'utilisation de la biométrie est le passeport. Ce document est une manière pour les Etats modernes de montrer leur monopole sur les moyens légaux de mouvements de leurs citoyens. Le document même du passeport constitue une technique d'expression de notre dégrée appartenance à une citoyenneté fournie par l'État.

Cette obsession d'attacher l'identité au corps transforme la notion de citoyenneté en gestion de l'identité. La citoyenneté a toujours été focalisée sur l'accès et les privilèges qui en découle. Aujourd'hui la reconnaissance faciale se soucie peu de qui nous sommes, ce qui compte c'est de savoir si nous sommes autorisés ou non à voyager ou accéder à une zone. Nous vivons dans une période où les mauvaises interprétations peuvent conduire à des erreurs difficilement rectifiables, comme le fait d'être ajouté

[56] D. Introna et H. Nissenbaum, *Facial Recognition Technology : a survey of policity and implementation issues*, p.46

sur une liste noire, ou avoir des impacts non négligeables, comme le fait d'être détenu à tort en garde à vue. De ce fait les voyageurs sont de plus en plus anxieux et douteux lors des passages de frontière et s'inquiète en se demandant « *sommes-nous l'identité attribué par l'Etat ou est-ce que l'Etat a mal interprété leur identité ?* ». Notre visage devient en quelque sorte un mot de passe.

1.2. Une initiative internationale face à peu d'opposition

Dans le DOC 9303, l'OACI a édicté des obligations en matière de photographie pour les passeports biométriques. Elle donne en outre des indications concernant la posture à adopter, les vêtements à ne pas porter et les coupes de cheveux conseillées afin de faciliter les procédures de reconnaissance de la personne.

En raison de la vocation sécuritaire de ce fichage généralisée, aucune alternative n'est laissée à la personne. Tout étranger voulant venir sur le territoire d'un Etat et tout citoyen dudit Etat voulant en sortir doit s'y conformer. Mis à part des refus individuels[57] qui se sont exprimés pour ne pas fournir leurs données biométriques, il n'y a pas eu de mouvement généralisé car les individus ne veulent pas être exclus de la mobilité transfrontalière

On remarque toutefois qu'il existe différentes conceptions de la liberté et la sécurité. La différence de conception découle de l'histoire des pays et des attentats qu'ils ont subis ou non, cela conduit à un décalage au niveau des programmes de biométrie. En l'absence de standard, le contrôle de biométrie faciale pourrait conduire à un déni d'identité dans un pays et à une acceptation dans un autre.

II. L'absence de standard international dans l'utilisation de la reconnaissance faciale.

2.1. La réaction de l'Europe face rôle actif des Etats-Unis.

Afin d'assurer une standardisation les Etats-Unis ont offert des subventions aux pays tiers, frontalière de l'Union européenne, pour qu'ils se dotent de leur système biométrique. Devenus vulnérables car ils ne peuvent plus « *identifier leurs*

[57] https://www.counterpunch.org/2003/01/23/italian-philosopher-giorgio-agamben-protests-us-travel-policies/

ennemis [58]», les Etats-Unis ont eu recours très rapidement à la reconnaissance faciale et à la biométrie d'une manière générale. C'est pour cela que les standards mis en place par le FBI et le NIST avait été utilisés par l'OACI pour les passeports biométriques. Le CBP utilise principalement aujourd'hui la reconnaissance faciale pour les entrées sur son territoire et souhaite étendre l'utilisation à 97% des départs internationaux d'ici 2022.

En Europe, la situation était très hétérogène avant l'adoption du règlement CE n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres. En effet, les autorités grecques par exemple, refusaient d'utiliser la biométrie comme méthode d'identification des voyageurs[59]. Avec l'adoption de ce texte, l'Union européenne a réussi à harmoniser les pratiques biométriques au sein de ses Etats membres.

2.2. Des visions différentes quant au stockage des données biométriques

Il existe également une différence de conception dans la manière de stocker les données biométriques servant à l'authentification. En effet, selon la CNIL et le G29, l'utilisation d'un support décentralisé pour vérifier l'identité est suffisant[60]. Utiliser une base de données centralisées créée à partir des procédures de délivrance des passeports et des visas serait excessive car la fonction principale d'une telle base de données est de lutter exclusivement contre la fraude documentaire.

Le Comité 108, crée par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, voit différemment. Selon lui, la finalité de sécurisation des titres ne peut pas être assurée sans l'aide d'un système d'identification reposant sur une base de données centralisée[61].
Par ailleurs, certains Etats par soucis de souveraineté comme la France ne délègue pas

[58] K. A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance (Critical Cultural Communication,* p.98
[59] https://transfert.net/La-Grece-bannit-la-biometrie-de
[60] Avis no 7/2004 du G29 sur l'insertion d'éléments biométriques dans les visas et titres de séjour prenant en considération la création du VIS.
[61] Rapport d'étape (1er février 2005) du comité consultatif de la Convention 108,

de compétence au groupe de travail du SC 37 (cf. supra) pour élaborer des documents normatifs internationaux relatifs à la gestion des données biométriques respectueuses de la vie privée et de la protection des données. C'est pourquoi ce groupe de travail fournis uniquement des rapports techniques aux Etats membres[62].

Aux Etats-Unis, la politique de confidentialité du CBP autorise la collecte des données biométriques pour identifier les individus et impose leur suppression après un délai de 12 heures. Néanmoins, cette disposition s'applique uniquement pour les citoyens américains[63].

Malgré ces différences dans la pratique, la reconnaissance faciale a réussi à se développer dans le monde entier. Aujourd'hui on compte 15 aéroports américains équipés de ce dispositif. En France, les aéroports de Roissy et d'Orly sont équipés de sas PARAFE à reconnaissance faciale depuis fin 2016, cette technologie s'est installée depuis à Lyon, Nice, Marseille et bientôt à Bâle-Mulhouse. La liste des pays utilisant cette technologie n'est pas exhaustive, mais on peut mentionner les pays comme la Chine, le Singapour, la Turquie, l'Australie.

[62] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 6 : *Les normes biométriques : réflexions sur le processus d'élaboration d'un corpus technique de portée internationale* par N.Delvaux, §23

[63] https://thehill.com/opinion/national-security/442722-biometrics-can-protect-our-borders-along-with-our-privacy

Chapitre 2 :
L'utilisation mondiale de la reconnaissance faciale pour le contrôle aux frontières

La reconnaissance faciale permet de renforcer le contrôle aux frontière car comme le précise Michael Williams (*Institutions of Security, 1999*), « *la migration a maintenu son rôle dans les agendas sécuritaires de plusieurs États puisque les médias et le gouvernement construisent le migrant, «* l'autre *», comme un danger pour la sécurité* »[64]. Par ailleurs, selon un rapport établi par Acuity Market Intelligence, le nombre de passage automatisé des frontières va tripler en passant de 1 100 en 2013 a 3 200 en 2018.

On constate donc que le recours à cette technologie a eu lieu dans un souci de contrôle de la migration (I), mais pour cela il est aussi nécessaire d'étendre le public pouvant bénéficier de la reconnaissance faciale (II).

I. La reconnaissance faciale en tant qu'outil de contrôle du flux migratoire.

1.1. L'uniformisation des pratiques européennes

Depuis l'entrée en vigueur du traité d'Amsterdam en 1999, l'Union européenne a une attention plus structurelle contre la migration irrégulière. D'ailleurs le champ lexical atteste de cette attention puisqu'on passe d'une « *politique d'immigration* » à « *la lutte contre l'immigration clandestine* ». Ainsi, l'Union européenne a investi dans une base de données biométriques pour l'immigration et certains Etats membres souhaitent étendre les finalités de cette base de données pour de la surveillance intérieure. Cette base de données est le Système d'information des visas (VIS).

Suite à la décision n°2004/512/CE du Conseil de l'Union européenne portant création du VIS, le Parlement européen a adopté le Règlement (CE) n° 767/2008 du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS). La Commission européenne dans sa décision n° 2006/648/CE du 22 septembre 2006 a précisé que le VIS ne créait pas de nouvelles normes techniques biométriques. En effet, pour les

[64] Benjamin J. Muller, (Dis)Qualified Bodies: Securitisation, Citizenship and 'Identity Management, p.4

visas, les normes employées renvoient à celles qui ont été développées par l'OACI dans son document 9303, qui a imposé des normes mondiales aux États pour certaines données biométriques (images faciales et empreintes digitales) devant être intégrées dans les documents de voyage.

1.2. Le changement de vision aux Etats-Unis

Aux Etats-Unis, le rapport d'enquête de la commission sur les attentats du 11 septembre 2001 avait défini les documents de voyage et contrôle d'identité comme des éléments clés du plan d'attaque des terroristes. D'après ce rapport, avant les attentats, « *la sécurité des frontières n'était pas considérée fondamentale à la protection de la sécurité nationale*[65] ». Ce même rapport indiquait que 15 des 19 terroristes étaient potentiellement vulnérables à un contrôle plus efficace des documents de voyage.

C'est également en 2016 que les Etats-Unis ont commencé à installer la reconnaissance faciale dans les grands aéroports du pays. L'objectif d'ici 2022 est d'équiper les aéroports avec cette technologie de sorte à pouvoir couvrir 97% des départs internationaux. Cette technologie aide les officiers dans leur travail, puisqu'ils n'auront plus besoin de se préoccuper du contrôle des documents mais peuvent se concentrer uniquement sur l'entretien avec le voyageur.

1.3. Les atteintes aux droit des individus causées par l'usage de la reconnaissance faciale

L'utilisation de la reconnaissance faciale peut remettre en cause les principes de liberté et d'autonomie. Restreindre le mouvement d'un individu est contraire aux dispositions de l'article 13 de la déclaration universelle des droits de l'Homme qui prévoit que : « *Toute personne a le droit de circuler librement et de choisir sa résidence à l'intérieur d'un Etat. Toute personne a le droit de quitter tout pays, y compris le sien, et de revenir dans son pays.* »

Une illustration de cette liberté entravée a eu lieu par exemple à l'aéroport Fresno de Yosemite aux Etats-Unis. L'aéroport utilisait un système de reconnaissance faciale qui avait un FAR de 1/750. Un passager déclenche cette alarme car la caméra l'identifie

[65] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (2004) http://govinfo.library.unt.edu/911/report/911lReport.pdf

comme suspect et il passe une nuit en garde à vue accompagné des agents du FBI car « *il ressemble à une personne originaire du Moyen-Orient* »[66]. Bien que dans les sociétés démocratiques la présomption d'innocence est supposée s'appliquer, le comportement du FBI a inversé la charge de la preuve dans la mesure où ils attendaient que le passager fournisse des preuves supplémentaires sur son identité et de son innocence. Le retenant ainsi pendant une nuit, il a été déni de sa liberté de mouvement et d'autonomie.

1.4. Les avantages avérés de la reconnaissance faciale

La reconnaissance faciale a permis de lutter plus efficacement contre les fraudes documentaires. En l'espace de trois mois, trois personnes ont été arrêtées à l'aéroport de Dulles (Washington) en 2018 grâce à la reconnaissance faciale car elles avaient des faux documents. Une femme qui prétendait être une ressortissante de Ghana s'est avérée être de nationalité camerounaise, un homme congolais avait utilisé un passeport français et une femme ghanéenne utilisait un passeport américain[67].

Par ailleurs, l'un des avantages majeurs de l'utilisation de la reconnaissance faciale est bien évidemment la réduction des durées d'attente lors des contrôles de passeport. En France, les sas PARAFE ont considérablement réduit temps de passage puisque les passagers mettent 10 à 15 secondes, contre 30 pour la reconnaissance digitale. Le gain de temps par rapport aux aubettes est plus marquant dans le sens où en général le temps passé par un officier de police à faire les vérifications est estimé à 1 minute. Par ailleurs, la reconnaissance faciale permet de toucher plus de passagers (45 %) que la détection par les empreintes (10 %), cette dernière étant limitée par la réglementation aux ressortissants français[68]. Les performances en terme du nombre de passagers traitées sont aussi en augmentation avec les sas PARAFE dernier cris, ils peuvent contrôler 300 passagers par heures.

[66] D. Introna et H. Nissenbaum, *Facial Recognition Technology : a survey of policity and implementation issues*, p.45

[67] https://wtop.com/loudoun-county/2018/10/facial-recognition-technology-at-dulles-catches-3-impostors-entering-us/

[68] https://www.challenges.fr/entreprise/la-verite-sur-les-sas-parafe-dans-les-aeroports_610257?refresh=1566307042999

La biométrie est utilisée pour tous les étrangers qui entrent sur le territoire américain, néanmoins concernant les sorties du territoire, les citoyens américains peuvent renoncer à l'utilisation de leurs données biométriques (*opting out*).

II. L'extension nécessaire de la reconnaissance faciale pour le contrôle aux frontière.

2.1. Un développement international ambitieux malgré des lacunes.

L'Australie est l'un des premiers pays au monde à utiliser la reconnaissance faciale pour l'entrée sur son territoire avec son programme *SmartGate*. Elle a commencé l'expérimentation à l'aéroport de Brisbane en 2007. Ce système était assez lacunaire dans ses débuts, puisqu'elle fonctionnait en deux étapes. Premièrement, il fallait que le passager passe devant une caméra qui prend sa photo (enrôlement) et qui émet un ticket. Ensuite, il se dirige vers un sas où il insert le ticket et là une deuxième caméra compare son visage avec celle prise au préalable. À la fin de sa première année, 100 000 personnes avaient utilisé ce système mais le FRR était très élevé (9%). Ceci s'explique par plusieurs raisons, notamment liées au passeport qui n'était pas conforme ou encore au passager qui n'avait pas suivi la procédure correctement.

Aujourd'hui, grâce aux *SmartGate*, l'Australie est devenue un modèle en matière de contrôle aux frontières. Un seul sas électronique peut traiter jusqu'à 150 passagers par heure, soit une personne toutes les 24 secondes dont la photographie numérique est stockée dans le passeport. Tous les titulaires d'un passeport biométrique peuvent utiliser les *SmartGate* à condition d'avoir 16 ans minimum. En effet, dans la plupart des pays les mineurs ne peuvent pas bénéficier des passages biométriques. Ceci étant, des projets sont en cours pour étendre la biométrie à tous les passagers, y compris les enfants. Soulignons également que c'est aussi en 2007 que la Grande Bretagne (*eGates*) et le Portugal ont décidé de déployer la reconnaissance faciale.

2.2. Un retard dans l'utilisation de la reconnaissance faciale en France

En France, ce sont les systèmes de Passage automatisé rapide aux frontières extérieures (PARAFE)[69] qui ont été mis en place depuis 2009 pour faciliter le passage

[69] Prévu par les articles R. 232-6 à R. 232-11 du code de la sécurité intérieure

aux frontière et assurer un meilleur contrôle des documents de voyage. Au début, les empreintes digitales assuraient l'identification de la personne, aujourd'hui le système s'oriente de plus en plus vers la reconnaissance faciale.

En effet depuis l'avis de la CNIL dans sa délibération n° 2016-012 du 28 janvier 2016 portant avis sur un projet de décret portant modification d'un traitement automatisé de données à caractère personnel dénommé PARAFE, les systèmes installés aux aéroports

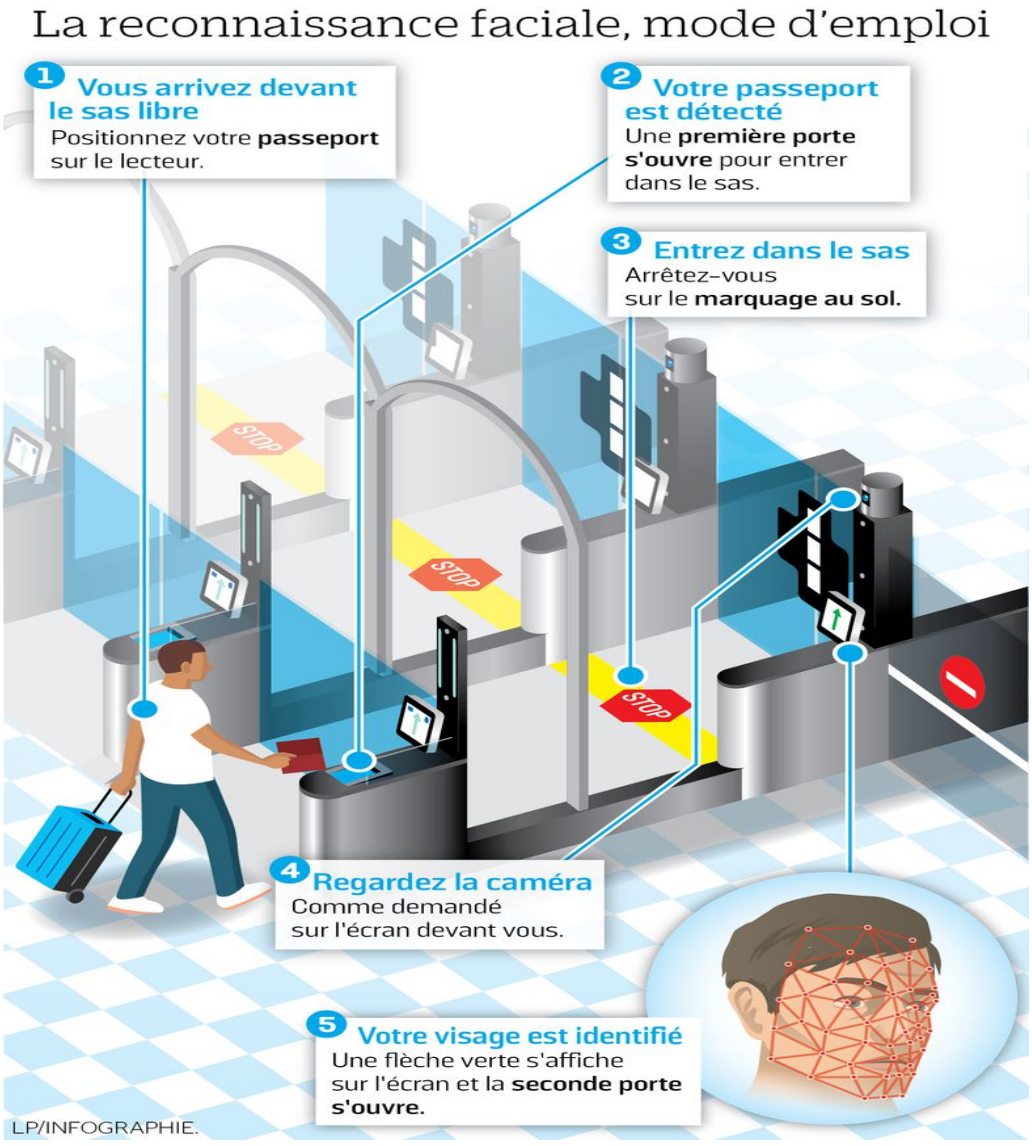

Figure 5 : Fonctionnement des systèmes PARAFE.
Source : http://www.leparisien.fr/economie/aeroports-de-roissy-et-d-orly-des-controles-par-reconnaissance-faciale-pour-embarquer-29-06-2018-7799964.php

sont autorités à traiter l'image de la personne pour vérifier son identité.

2.3. Des restrictions affaiblissant l'utilisation de la reconnaissance faciale.

2.3.1. L'extension entamée des bénéficiaires de la reconnaissance faciale

L'accès au système PARAFE est restreint aux passagers majeurs, titulaires d'un passeport biométrique et ressortissants d'un des 28 pays de l'Union européenne, de la Suisse, de l'Islande, de la Norvège ou du Liechtenstein. Les passeports diplomatiques ne sont pas éligibles non plus, l'exemple le plus concret a été celui de l'ancienne ministre des transports Elisabeth Borne qui a été refusée d'accès par les sas PARAFE lors de leur inauguration à Orly, le 6 juillet 2018. D'ailleurs, la caméra peut parfois scanner par erreur un visage imprimé sur un tee-shirt ou être perturbée par une trop forte luminosité

CNIL a émis un avis favorable le 29 mars 2019 dans sa délibération n° 2019-027 pour l'extension des PARAFE aux enfants de 12 ans révolus et aux ressortissants de Monaco, Andorre et aux ressortissants de pays tiers détenteurs d'une carte de séjour de membre de la famille d'un citoyen de l'Union européenne prévue par l'article 10 de la directive 2004/38/CE émise par le France ou par un autre Etat membre de l'Union européenne et en cours de validité. La CNIL rappelle son opposition à une base de données centralisée en indiquant que « *elle considère comme légitime le recours à des dispositifs de reconnaissance biométrique pour s'assurer de l'identité d'une personne, dès lors que les données biométriques sont conservées sur un support dont la personne à l'usage exclusif, comme c'est le cas pour le passeport biométrique* ». Quand bien même la durée de conservation des données est de 5 ans, elle estime que pour les mineurs ce délais doit être réduit à 3 ans dans la mesure où, conformément à l'article 38 de la RGPD, les enfants doivent bénéficier d'une protection spécifique.

2.3.2. Le doute persistant des agents de la Police aux frontières

Avant même l'utilisation de la reconnaissance faciale, une étude menée à Roissy au sein des agents de la Police aux frontière (PAF) en 2005[70] avait conclu que l'âge et la formation sont des critères qui jouent sur l'acceptabilité des nouvelles technologies.

[70] A.Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 20, *« Acceptabilité » de la biométrie : linéaments d'un cadre analytique,* §18

Ainsi, plus on est jeune plus on est enclin à utiliser les solutions biométriques. Les plus âgés évoquaient notamment comme cause de leur réticence le manque d'efficience et le niveau de performance des solutions biométriques.

Aujourd'hui, les agents de la PAF semblent toujours aussi dubitatifs à l'utilisation des outils biométriques à cause des heures de travail qui sont de plus en plus longues et des systèmes informatiques qui tombent sans cesse en panne[71]. D'autant plus que compte tenu des attentats des dernières années sur le territoire français, les contrôles sont plus approfondis aux frontières. La solution serait donc de mettre à disposition plus d'agents de police sachant que le trafic aérien n'est pas prêt de ralentir sa croissance.

[71] https://www.challenges.fr/entreprise/la-verite-sur-les-sas-parafe-dans-les-aeroports_610257?refresh=1566307042999

Conclusion sur la première partie :

Le développement de la reconnaissance faciale est fortement poussé par les autorités qui souhaitent établir un contrôle plus efficace de la population tant pour la sécurité intérieure que pour le renforcement des frontières. On constate que la protection des libertés individuelles semble peser faiblement face aux discours économique et sécuritaire. La ministre de l'immigration Amanda Vanstone affirme comprendre l'inquiétude des individus, mais renvoie la faute aux studios d'Hollywood pour leurs interprétations erronées : « *Je ne pense pas avoir vu de film qui démontre la biométrie comme étant au service des personnes faussement accusées* »[72].

Les différents gouvernements dans le monde ont ainsi contribué ainsi à financer la recherche et le développement dans ce domaine de la biométrie faciale. Aujourd'hui, grâce aux avancées dans l'intelligence artificielle ou encore dans l'utilisation des réseaux de neurone, la reconnaissance faciale est une technologie globalement fiable malgré les taux d'erreur variables d'un pays à l'autre.

La confiance envers cette technologie pousse même les entreprises privées ou publiques à s'équiper de caméra de reconnaissance faciale dans le cadre de leurs activités. Parmi elles, encore une fois, les aéroports ont un rôle central. Ces derniers peuvent utiliser la reconnaissance faciale pour améliorer l'expérience passager mais aussi pour contrôler les accès et sorties en ZSAR.

[72] Benjamin J. Muller, (Dis)Qualified Bodies: Securitisation, Citizenship and 'Identity Management, p.6

Partie 2 :
L'utilisation de la reconnaissance faciale par le gestionnaire aéroportuaire : amélioration de l'expérience passager et gestion des accès.

Les gestionnaires d'aéroport collaborent étroitement avec les compagnies aériennes afin de mettre en place des facilitations pour rendre plus agréable l'expérience du passager au sein de l'aérogare. En effet, la plupart des passagers sont souvent sous l'effet de stress lié à la peur de rater son vol ou à la peur de l'avion et du voyage en avion (*l'aviophobie*).

Les contraintes de sûreté aéroportuaire n'améliorent en aucun cas cette expérience car les voyageurs deviennent plus tendus lors des passages au PIF. Pour réduire ce stress et faire gagner du temps au passager, les aéroports à travers le monde investissent dans la biométrie et dans la reconnaissance faciale, améliorant ainsi l'expérience du passager (**Titre 1**).

Les infrastructures aéroportuaires représentent également une taille importante en terme de personnel, l'aéroport de Roissy Charles de Gaulle compte 88 600 salariés. Avec la croissance du trafic aérien, le nombre d'emplois dans le domaine aéroportuaire va nécessairement augmenter. D'autant plus que le rôle stratégique des aéroports fait que tout salarié n'a pas accès à toutes les zones. La reconnaissance faciale permet ainsi d'optimiser la gestion des accès sur le site de l'aéroport (**Titre 2**).

Titre 1 :
L'amélioration de l'expérience du passager grâce à la reconnaissance faciale.

La facilitation du passage au sein de l'aérogare permet au voyageur de subir moins de stress et de gagner du temps. La réduction du temps de passage du voyageur pourrait également réduire le temps d'embarquement pour les aéronefs lors des correspondances ou des rotations. C'est pour cela que les aéroports collaborent étroitement avec les compagnies aériennes (**Chapitre 1)** dans l'installation des dispositifs de reconnaissance faciale.

Ce gain de temps pourrait éventuellement pousser le voyageur à effectuer des achats au sein de l'aérogare et l'aéroport aura donc intérêt à capter cette clientèle qui, sans correspondance, tend en général à réduire le temps passer dans l'enceinte de l'aérogare. C'est pour cela que de nombreuses initiatives émanant des gestionnaires aéroportuaires se développent (**Chapitre 2**).

Chapitre 1 :
Une collaboration étroite entre les compagnies aériennes et les aéroports

Les compagnies doivent logiquement coopérer avec les aéroports pour la mise en place de système biométrique puisque ces derniers agissent en tant qu'interface entre la compagnie et les passagers. Les deux entités travaillent étroitement pour la mise en place « *seamless travel* » (I), mais on remarque que les compagnies aériennes veulent pousser l'utilisation de la reconnaissance faciale plus loin (II).

I. Le développement du concept de « *seamless travel* ».

Suite à une enquête menée en 2018 aux Etats-Unis, 1 voyageur sur 7 dit avoir raté son vol à cause des longues files d'attente dans les contrôles de sureté.[73] Le terme de « *seamless travel* » correspond en français au « voyage sans rupture ». C'est un concept qui se développe pour faciliter le déplacement du passager au sein de l'aéroport. D'ailleurs, cette expression tend à remplacer le terme « d'expérience passager » et cela se comprend car ces deux éléments renvoient à des pratiques différentes. Ainsi, lorsqu'on parle de « *seamless travel* », il s'agit d'offrir au voyageur une expérience sur mesure en fonction des données que ce dernier est prêt à fournir. Tandis que dans l'expérience passager, on développe une stratégie commune pour tous les voyageurs.

La meilleure manière d'établir le voyage sans rupture est de recueillir des données personnelles et biométriques des passagers. On remarque aujourd'hui que 71% des compagnies aériennes investissent dans la biométrie tandis que ce chiffre est de 77% pour les aéroports[74]. L'adoption du RGPD a également facilité cet investissement en biométrie dans la mesure où aujourd'hui, notamment en France, l'obligation n'est plus d'obtenir le consentement de l'individu mais de lui fournir de manière claire et précise les informations concernant le prélèvement et le traitement de ses données. En effet, le respect des principes de libertés individuelles et de la vie privée impose que la finalité

[73] https://www.forbes.com/sites/garystoller/2018/06/26/one-of-every-seven-travelers-miss-their-flights-because-of-long-airport-security-lines/#55ef0a352e1d

[74] Business Traveler, article de J. Reid, *Airport facial recognition : What you need to know,* publié le 09/06/2019

d'un traitement soit définie de façon précise pour apprécier la proportionnalité au regards des objectifs poursuivis.

Puisque l'établissement d'une base de données centralisée suscite beaucoup de débats et est vu d'un mauvais œil par les autorités de protection des données, les compagnies aériennes et aéroports privilégient l'utilisation d'un support de stockage détenu par l'individu. En plus d'une meilleure protection de données, le coût d'un tel support serait moindre que celle d'une base de données centralisée. En effet, il n'y aurait plus besoin de recourir à d'immense serveur qui nécessitent un entretien et une mise à jour régulièrement. D'ailleurs, le coût du support individuel peut être rentabilisé avec une participation financière de la part du voyageur.

En juin 2019, lors du 75^{e} sommet de l'IATA, des discussions s'articulaient autour de l'accélération dans l'adoption du One ID pour faciliter les déplacements du voyageur. Le One ID est en outre le projet lancé par l'IATA pour réaliser le « *seamless travel* ». Compte tenu de l'augmentation croissante du nombre de passager, mais aussi des contraintes de sûreté et des limites dans les expansions des infrastructures, il faut développer des méthodes permettant de fluidifier le passage des voyageurs pour mieux gérer les défis futurs. Le One ID vise également de permettre au voyageur de bénéficier d'un contrôle de sûreté adapté et moins contraignante.

Récemment, la solution IDEMIA nommée ID2Travel a été testée avec la collaboration d'Air France et ADP. Selon cette méthode, le passager dispose de deux choix : après avoir fait son check-in en ligne ou à l'aérogare, il peut enregistrer ses données biométriques dans sa carte d'embarquement ou utiliser ses empreintes digitales et son visage en tant que carte d'embarquement, sachant que cette deuxième situation nécessitera la sauvegarde des données dans une base centralisée. Par la suite le parcours du passager se fluidifie car il n'a plus à présenter de document accédant ainsi à la salle d'embarquement, passant les frontières sans montrer de document de voyage. Il peut également accéder aux salons VIP et enfin procéder à l'embarquement. La proposition d'IDEMIA pour le « *seamless travel* » intègre aussi le paiement dans les duty-free, la location de voiture ou la réservation d'hôtel.

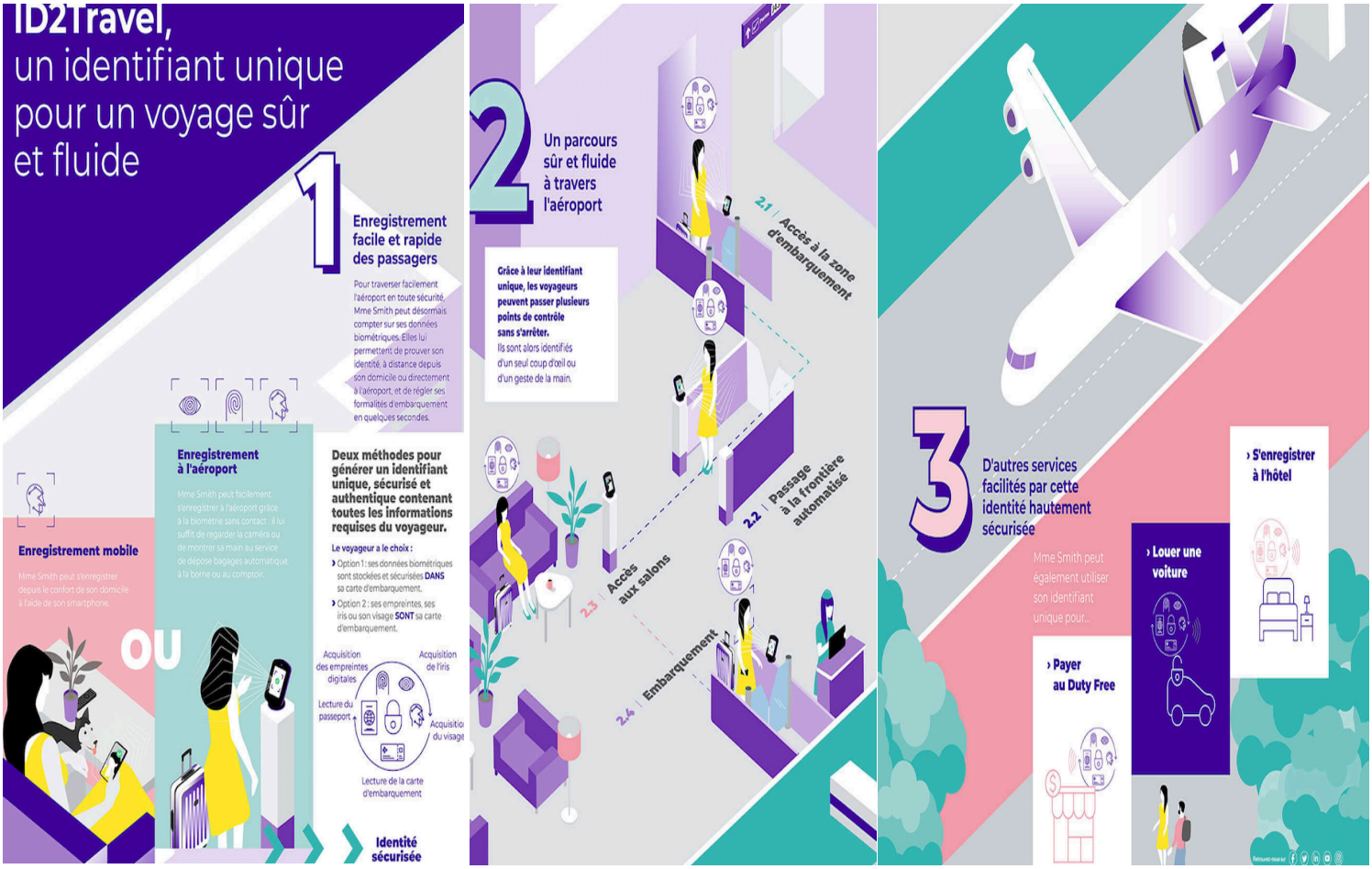

Figure 6: Solution ID2Travel proposée par IDEMIA –
Source: https://www.idemia.com/fr/actualite/infog-id2travel-un-identifiant-unique-pour-un-voyage-sur-et-fluide-2019-06-11

Néanmoins se pose un problème d'accessibilité qu'il convient de souligner. Bien que la probabilité soit plus faible aujourd'hui, des catégories de personnes (cf. supra FTE et FTA) ne peuvent pas être enrôlées car elles ne possèdent pas les caractéristiques corporelles exigées ou que celles-ci ne soient pas lisibles par la machine. C'est pourquoi il serait plus logique de conserver les méthodes traditionnelles de voyage aux cotés de la « *seamless travel* » afin d'assurer une continuité du service pour tous les voyageurs.

II. La volonté des compagnies aériennes pour l'utilisation généralisée de la reconnaissance faciale.

L'Annexe 9 – Facilitation de la Convention de Chicago de 1944 recommande dans son article 3.9 l'intégration des données biométriques dans les DVLM pour faciliter

l'expérience du passager. En effet depuis un amendement de 2004, l'utilisation des données biométriques font partie de l'Annexe 9 – Facilitation. Depuis ce changement, les compagnies aériennes et les aéroports se sont mobilisés pour utiliser ces techniques biométriques.
L'empreinte digitale était privilégiée au début, mais au fur et à mesure des avancements dans la technologie, la reconnaissance faciale semble prendre le dessus.

2.1. Les utilisations mondiales de la reconnaissance faciale

D'après l'enquête réalisée auprès des passagers par IATA en 2018, les passagers sont favorables à l'utilisation de la reconnaissance faciale si cela réduit leur temps d'attente[75]. De ce fait plus le temps passe, plus les exemples de compagnies aériennes utilisant la reconnaissance faciale se multiplient.

Dès 2010, la compagnie British Airways a commencé à utiliser la reconnaissance faciale pour les passagers des vols internes avec un service de self-boarding. En 2017, plus de 3 millions de voyageurs avaient bénéficié de ce service. En décembre 2017 elle a commencé à utiliser la reconnaissance faciale à Los Angeles (LAX) avec l'accord des autorités américaines, puis a développé la même pratique à Orlando (MCO) en Floride et à New York (JFK). Depuis mai 2019, le terminal 5 de l'aéroport Londres-Heathrow est équipé de machines biométriques pour les vols internationaux[76] effectués par British Airways.

En Europe, on peut mentionner l'exemple de Adria Airways et LOT Polish Airlines qui, en mai 2019, ont testé le boarding biométrique à l'aéroport de Ljubljana en collaboration avec Amadeus, où les smartphones ont servi de support de stockage des données biométriques. Le gain de temps a été remarquable puisque la machine ne prenait que 2 secondes pour authentifier un passager.

Du côté des américains, Delta Airlines et JetBlue utilisent eux aussi la reconnaissance faciale depuis l'automne 2018 tandis qu'American Airlines a commencé en décembre 2018. Par ailleurs, Delta Airlines a indiqué son intention d'étendre la reconnaissance

[75] https://www.arabianaerospace.aero/how-technology-is-making-aviation-safer.html
[76] http://www.ba-groups.com/about-groups-travel-hub/news/02-05-2019/british-airways-introduce-biometric-technology.aspx

faciale sur 49 portes d'embarquement dans ses hubs situés à Atlanta, Minneapolis et Salt Lake City pour les vols internationaux. En effet, selon une enquête réalisée par la compagnie, 72% des passagers préfèrent l'embarquement avec la reconnaissance faciale. Le développement de cette technologie permet à Delta de gagner jusqu'à 9 minutes dans les embarquements des aéronefs gros porteurs.

L'aéroport de Tokyo Narita va être la première à introduire une application complète du One ID au printemps 2020. Au début, le nombre de compagnie bénéficiaire va être restreint à South Wing et All Nippon Airways dans le Terminal 1 et à la Japan Airlines dans le Terminal 2. L'extension aux autres compagnies aériennes aura lieu ultérieurement, étape par étape.

2.2. La remise en cause du passeport.

Lors de son sommet en juin 2019, l'IATA a lancé un appel aux compagnies aériennes, aux aéroports, aux autorités gouvernementales et à toutes les parties prenantes pour implanter des procédures de voyages sans documents physique, en utilisant la biométrie. Selon elle, avec le déploiement de la biométrie on peut libérer jusqu'à 40% d'espace au sein d'un terminal.

Les compagnies aériennes ont entre autres invité les Etats membres de l'OACI d'incorporer les méthodes de voyages biométrique comme le OneID en tant qu'alternative au passeport[77]. De plus, il revient également aux industriels de l'aviations et aux Etats de travailler étroitement pour développer des standards mondiaux afin de sécuriser, transférer et utiliser les données d'identité du voyageur sur une base de « besoin » ou « d'autorisation ». Tout cela évidemment doit s'inscrire dans le cadre des règlementations par rapport au respect de la vie privée des individus. Le premier exemple d'une telle collaboration a eu lieu avec le Canada et les Pays-Bas avec les tests du KTDI.

[77] https://www.biometricupdate.com/201906/iata-unanimously-resolves-to-speed-adoption-of-one-id-for-biometric-air-travel?

2.3. Les menaces liées à la récolte des données biométriques

Nous savons que les Etats relevant de l'Union européenne sont déjà soumis au même principe de protection avec le RGDP, mais certains pays comme les Etats-Unis ne connaissent pas un niveau de protection équivalent. Suite à la directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers un accord a été trouvé en 2007 entre l'Union européenne et les États-Unis sur le traitement et le transfert de données des dossiers passagers (données PNR – *Passenger Name Record*) par les transporteurs aériens au *Department of Homeland Security* (DHS).

Le Conseil de L'Union européenne a adopté la directive relative aux données des dossiers passagers le 21 avril 2016. Cette directive vise à réglementer le transfert vers les États membres, par les compagnies aériennes, des données PNR des passagers des vols internationaux, ainsi que le traitement de ces données par les autorités compétentes.

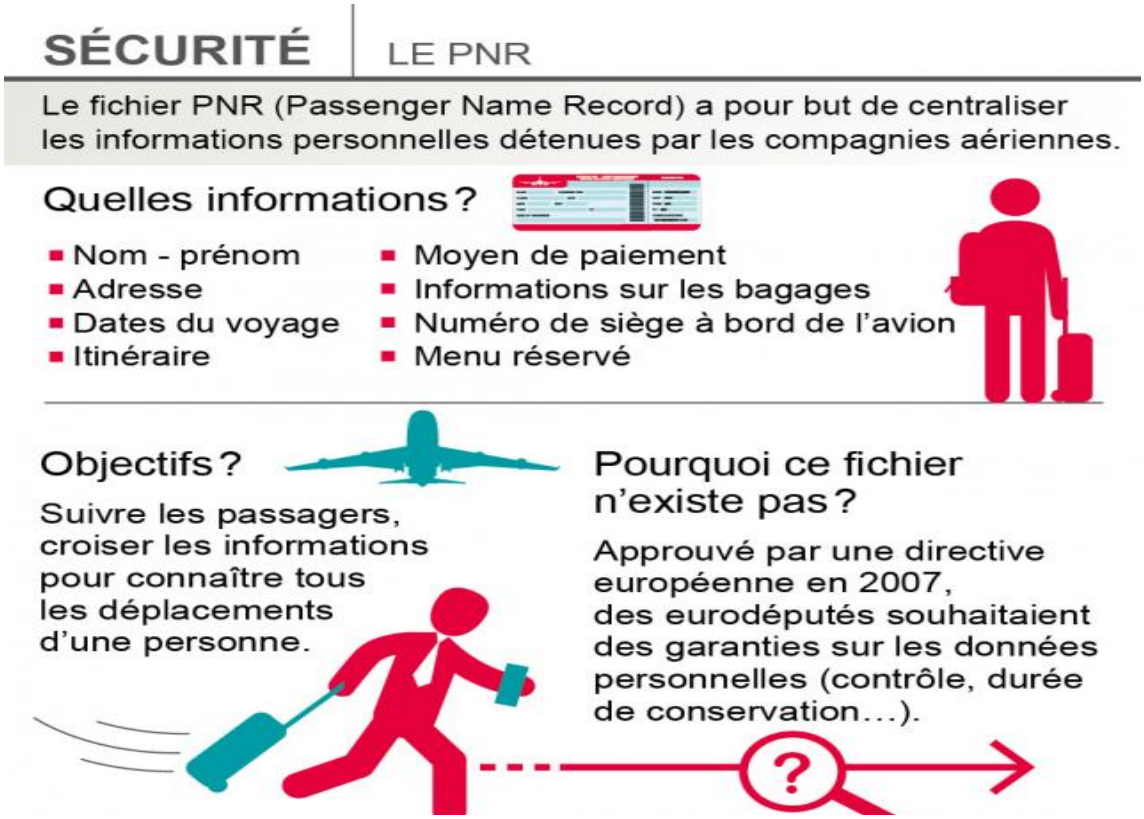

Figure 7 : Explication du PNR et de l'échange des données.
Source: https://www.ouest-france.fr/societe/faits-divers/attentat/attentats-bruxelles/ladoption-du-pnr-en-bonne-voie-au-parlement-europeen-4162801

Toutefois, une limite est posée par la directive qui indique que les données recueillies ne peuvent être traitées « *qu'aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière* ».

La question qui se pose aujourd'hui est de savoir si le domaine d'application de ces accords ne serait pas étendu avec le One ID et le « *seamless travel* » puisque ce dernier stock les données également les données biométriques, or l'échange de ces données n'est pas prévu dans les accords initiaux.

Un autre problème provient du risque de « *data-mining* » qui a pour objet l'extraction d'une connaissance à partir de grandes quantités de données (exploration de données). Ainsi, les compagnies aériennes utilisant les outils biométriques pourront utiliser les données biométriques pour d'autres finalités comme connaître l'origine des passagers, et suivre leur comportement.

La menace d'une cyberattaque n'est pas à sous-estimer non plus, les établissements aéroportuaires ou les compagnies aériennes sont souvent des cibles privilégiées. Les hackeurs pourront facilement accéder à un éventail beaucoup plus large de données sensibles et personnelles sur des millions d'individus. Il faut mettre en place des systèmes sécurisés de sorte à ce que seul le gouvernement puisse avoir accès à ces données et ce sous conditions prévue par la loi.

Face à l'utilisation massive des technologies biométriques, les aéroports investissent eux aussi dans des projets pour bénéficier des avantages de la technologie. Ainsi, la reconnaissance faciale n'est pas utilisée uniquement pour l'embarquement dans le sens où les aéroports innovent en la matière et fournissent d'autres services basées sur la reconnaissance faciale.

Chapitre 2 :
La diversification des initiatives aéroportuaires utilisant la reconnaissance faciale

D'après les enquêtes[78], 77% des aéroports investissent dans les nouvelles technologies biométriques et sont de plus en plus connectés grâces aux NTIC (I). Afin de bénéficier des avantages de la reconnaissance faciale, les aéroports proposent des utilisations secondaires de la technologie qui ne servent pas qu'à l'embarquement ou à l'authentification de l'individu (II).

I. Des aéroports de plus en plus connectés

1.1. Le développement des aéroports intelligents

On assiste aujourd'hui à un mouvement dans les aéroports qui est celui de la multiplication des connectivités. Cette tendance s'explique par la volonté des aéroports de mettre en place les outils nécessaires au déploiement de l'initiative OneID mais aussi de bénéficier des retombés économiques qui découlent de l'utilisation des NTIC. Les vecteurs principaux dans l'utilisation de la connectique sont les suivants :

- La rapidité de l'expérience voyageur : il faut faciliter la capture et l'utilisation des données biométriques de qualité et ainsi rendre plus agréable l'interaction du passager lors de son déplacement au sein de l'aérogare.
- La performance et la précision : Les outils biométriques fonctionnent dans un environnement automatisé, ainsi leurs performances peuvent être facilement mesurées et l'analyse des résultats peut être plus rapide
- L'intégration : Il faut avoir une intégration étroite entre les caméras de capture et les algorithmes de correspondances

Par rapport aux initiatives aéroportuaires, on peut citer par exemple l'aéroport de Doha (Hamad) au Qatar qui a développé le « *Smart Airport Programme* » qui vise à aider le voyageur dans ses déplacements. L'aéroport a notamment développé une application

[78] https://www.businesstraveller.com/features/airport-facial-recognition-what-you-need-to-know/

pour smartphone qui permet au passager d'enregistrer sa carte d'embarquement et de retrouver sa porte d'embarquement grâce à un itinéraire qui s'affiche sur son écran.

L'aéroport de London Heathrow, cité auparavant avec l'analyse de British Airways, a aussi investi 50£ millions de livre sterling dans le « *seamless travel* ». Sur son site internet, l'aéroport indique que la reconnaissance faciale est encore sous test et invite les passagers volontaires à s'inscrire sur une liste pour bénéficier des avantages de la biométrie faciale[79]. L'aéroport de Lisbonne utilise également la reconnaissance faciale pour l'enregistrement et l'embarquement des passagers avec la solution Vision BOX.

L'aéroport de Changi à Singapour collabore avoir IDEMIA depuis l'ouverture de son terminal 4 en octobre 2017. Grâce à cet investissement, 6 millions de passagers ont été accueillis et tout en réduisant les files d'attente et les ressources déployées pour gérer le flux des passagers.

Le but est de confirmer l'identité des personnes sans interrompre le flux des passagers et améliorer les outils à dispositions au lieu d'agrandir les infrastructures. Ceci se reflète par la suite en tant que satisfaction du client dans les enquête ASQ.

1.2. Une collaboration embryonnaire entre Etats et acteurs privés.

L'initiative que nous pouvons mentionner ici est le projet du « *Known Traveler Digital Identity* » (KDTI) développé par le Canada et Pays Bas. Il s'agit d'un partenariat entre les deux Etats qui vise à supprimer l'utilisation des documents physiques en stockant toutes les données sur l'appareil mobile du voyageur. Ainsi, les passagers peuvent choisir le moment et l'autorité avec laquelle ils souhaitent partager leurs données personnelles (compagnie aérienne, aéroport, police aux frontières).

Au fur et à mesure de leur passage dans les enceintes aéroportuaires, les voyageurs accèdent à un statut dit de « voyageur connu » et les données accumulées sont vérifiées par des partenaires utilisant la plateforme de l'aérogare. Les test pilotes ont été effectués avec les compagnies Air Canada et KLM aux aéroport de Montréal-Trudeau, Toronto-Pearson et Amsterdam-Schipol. Les technologies biométriques utilisées ont

[79] https://www.heathrow.com/departures/security-and-baggage/biometric-testing

été fournis par la société Accenture en partearіat avec d'autres fournisseurs comme Vision Box ou IDEMIA.

La ministre de l'immigration des Pays-Bas, Mme Ankie Broekers-Knol, indique que « *Le projet KTDI est l'exemple parfait d'un partenariat entre acteur privés et public dans l'innovation du secteur de l'aviation* » puisque le but étant de faciliter le voyage du passager sans pour autant compromettre la sécurité des frontières.

Aux Etats-Unis, l'agence de la Transportation Security Administration (TSA) permet d'écourter les attentes dans les aéroports avec une autre initiative. En payant une somme de 85$ pour 5 ans, on devient membre du programme du TSA qui nous permet de conserver nos chaussures et la ceinture, mais aussi nos ordinateurs portables et les liquides dans le sac sans avoir à les sortir au moment des contrôles de sûreté. Pour cette suscription, il faut néanmoins fournir des données personnelles comme l'image afin que l'on puisse être identifié par la caméra lors du passage aux PIF. D'après les chiffres du TSA, 92% des membres ont attendu moins de 5 minutes dans la file d'attente en mai 2018. Le programme compte aujourd'hui plus de 6 millions de membres et opère sur plus de 200 aéroports américains.

II. Les utilisations secondaires envisageable de la reconnaissance faciale

Mis à part la fluidité des déplacements au sein de l'aérogare, la reconnaissance faciale peut également avoir d'autre utilité. Par exemple en Chine, l'aéroport de Chengdu Shuangliu (province du Sichuan) est équipé d'un système de reconnaissance faciale qui permet avec l'image du visage de nous donner des indications sur notre vol comme le numéro des bornes d'enregistrement, le numéro des portes d'embarquement ou encore les retards. La Chine est un leader mondial dans la technologie de reconnaissance faciale, mais son utilisation de la technologie laisse les individus assez perplexes car le gouvernement chinois est accusé de créer un système de surveillance avec les données collectées par la reconnaissance faciale pour retrouver les membres de la minorité Ouïghours notamment.

Une autre utilisation de la reconnaissance faciale peut être envisagée pour les bagages abandonnés. En effet des travaux en ce sent ont été menés avec des évolutions considérables. Dans les recherches de Ziyan Wu & Richard J Radke « *Real-Time*

Airport Security Checkpoint Surveillance Using a Camera Network » (Juin 2011) ces derniers nous expliquent que les systèmes précédents utilisaient une technique particulière pour retrouver les propriétaires des valises abandonnées. L'algorithme retraçait l'historique de toutes les séquences enregistrées par la caméra pour retrouver le propriétaire de la valise.

Aujourd'hui, leurs travaux permettent de rechercher en direct les propriétaires des bagages de la manière suivante[80] : la caméra de surveillance crée « une goute » autour du passager et arrive à faire la distinction entre ce dernier et les agents de sûreté. L'alarme se déclenche lorsque la valise reste figée pendant plusieurs images. Les tests avaient été effectués dans un scénario précis, au moment du passage des contrôles de sûreté. Les résultats de ces tests sont assez satisfaisants, car il n'y a eu que 3 fausses alarmes dont l'un s'explique par le fait que la caméra a considéré un bac comme une valise car le passager l'avait empilé sur un autre bac.

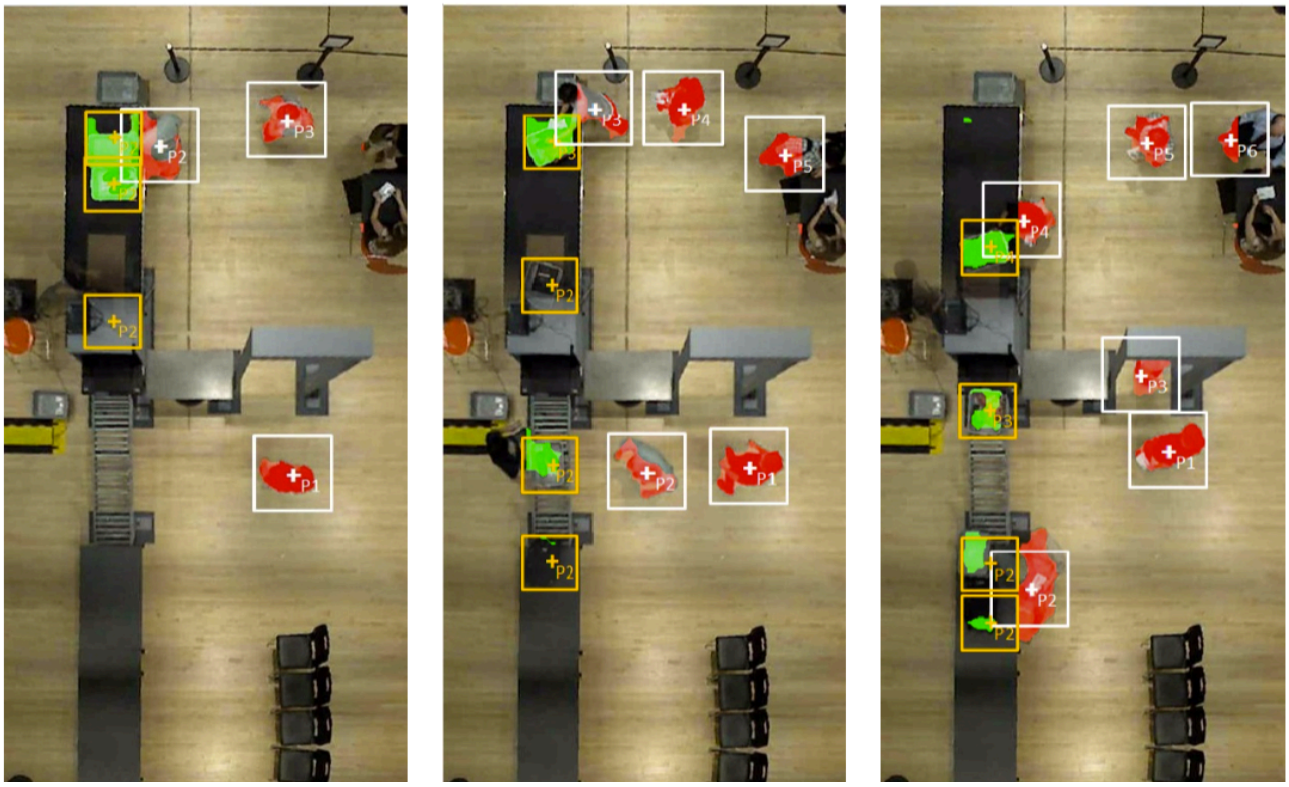

Figure 8 : Capture d'écran de la caméra effectuant le rapprochement entre les valises et les voyageurs.
Source : Real-Time Airport Security Checkpoint Surveillance Using a Camera Network (Juin 2011), Z. WU & R. J. Radke

[80] Pour l'illustration vidéo des tests : https://www.youtube.com/watch?v=BpxGXTcayBs

Enfin, les informations tirées de la reconnaissante faciale peuvent permettre de renforcer une fouille basée sur le risque. Le concept de cette fouille repose sur le principe de différenciation des passagers en appliquant des procédures de fouilles appropriées. Cette différenciation se base sur un score de risque qui provient des analyses de leurs destinations ou de leurs données personnelles. L'utilisation de la reconnaissance faciale réduit le travail des agents de sûreté et augmente la qualité de leurs services.

Il faut rappeler également que conformément aux différentes règlementations, notamment le RGPD, les données collectées doivent être conservées pour une durée limitée et supprimées par la suite. Le passager doit toujours être informé des traitements effectués sur ses données personnelles et doit avoir la possibilité d'opting out pour ne pas s'y soumettre.

La reconnaissance faciale peut être utilisée tout au long du parcours du passager (check-in, sûreté, achats, passage aux frontière et embarquement). Mais cette technologie peut aussi permettre de mieux contrôler les accès en zones de sûreté à accès règlementé (ZSAR).

Titre 2 :
L'optimisation de la gestion d'accès grâce à la reconnaissance faciale

Le contrôle d'accès en zone de sûreté se déroule de la même manière que les passagers, c'est à dire que le personnel doit passer par un PIF ou PARIF. N'ayant pas de titre de transport, les employés doivent être munis de leur badge qui leur donne accès en ZSAR.

Compte tenu du nombre important d'employés sur un site aéroportuaire, gérer leur accès devient de plus en plus compliqué en terme de logistique, c'est pourquoi des aéroports ont recours à de nouvelles technologies biométriques, dont la reconnaissance faciale. Celle-ci permet de renforcer la sécurité des accès en ZSAR (**Chapitre 1**) mais il faut garder à l'esprit que le respect de la finalité attribuée fait l'objet d'un contrôle très strict (**Chapitre 2**).

Chapitre 1 :
Le renforcement de la sécurité des passages en zone de sûreté à accès réglementé

La reconnaissance faciale permet d'améliorer le contrôle de sûreté (I) dans le sens où elle donne la possibilité à l'agent de sûreté de se concentrer sur sa tâche principale de fouille et de palpation. Toutefois, l'utilisation de cette technologie nécessite une standardisation dans la protection des données stockées (II).

I. Un contrôle de sûreté amélioré

Le choix d'un système de biométrie au lieu d'une autre doit se baser sur des considérations de capacités, restreintes et facteurs techniques ou moraux. La caméra de reconnaissance faciale a fait ses preuves avec les exemples démontrés jusqu'à maintenant. Dans son utilisation en tant qu'outil de gestion d'accès en ZSAR, elle permet de vérifier l'identité du salarié.

Les agents de sûreté présents sur place n'auront plus besoin d'effectuer de vérification d'identité et pourront se concentrer sur d'autres tâches notamment liées aux palpations et fouilles. Réduisant leur travail, la reconnaissance faciale permet également de pallier les problèmes liés aux manques d'effectif au sein des équipes de sûreté.

Plus concrètement, le déroulement de cette procédure s'effectue de la manière suivante : l'employé passe par le PIF puis se met en face de la caméra qui affiche une lumière en fonction du résultat obtenu (Vert si l'employé est reconnu et a le droit d'accès, rouge si l'employé n'est pas reconnu ou n'a pas droit d'accès). Afin de lutter contre les techniques de fraudes, il est possible d'installer dans le logiciel de la caméra un détecteur de « *liveness* ». Le principe est simple, en plus de reconnaître la personne, la caméra détectera si l'image qu'elle traite appartient à une personne vivante et n'est pas une tentative de fraude (image imprimée ou masque).

La pertinence de cette technologie de « *liveness* » pour les PIF est discutable dans la mesure où, conformément au règlement n°2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de

base communes dans le domaine de la sûreté de l'aviation civile, un agent de sûreté doit être toujours présente pour contrôler le passage d'un employé.

Toutefois, cette technologie prend de l'importance lorsqu'on veut généraliser la reconnaissance faciale à l'ouverture des portes. Ainsi, bien que ce soit en zone publique, les portes menant notamment aux bureaux des aéroports sont accessibles à l'aide badge. La possibilité d'ouvrir des portes à l'aide de la reconnaissance faciale peut augmenter le risque de fraude et une personne mal intentionnée qui entre dans les bureaux pourrait causer des dommages importants (vols d'informations, dégâts du matériel, perturbation du travail etc…). C'est pourquoi le FAR en terme d'accès peut être de 1/10 000, ce qui est beaucoup plus élevé que le seuil nécessaire pour l'authentification des passagers dans les sas PARAFE.

II. Une standardisation nécessaire dans la protection des données stockées.

Pour que la reconnaissance faciale puisse fonctionner correctement, il faut que la base de données soit mise à jour. Cette actualisation doit se faire à rythme régulier dans la mesure où la mobilité des employés (embauche/démission) peut-être intense notamment durant les hautes saisons de l'aéroport.

Dans le cas justement de gestion d'accès, on peut estimer qu'un impératif de sécurité justifie la mise en place d'une base de données centralisée. Mais il n'existe actuellement aucune loi ou réglementation quant aux méthode de sécurisation des données enregistrées.

Les seules mesures qui se rapprochent d'une forme de « sécurisation » sont celles liées à la limite dans la durée de conservation des données biométriques. En effet, les données biométriques étant des données sensibles, leur conservation doit être limitée dans le temps, contrairement aux autres données personnelles comme le nom et l'adresse qui peuvent être conservés pendant 5 ans après le départ de la personne de l'entreprise.[81]

[81] CNIL, délibération n° 2012-243 du 12 juillet 2012 autorisant la société EMC COMPUTER SYSTEMS FRANCE à mettre en œuvre un traitement de données à caractère personnel reposant sur un procédé de reconnaissance vocale et ayant pour finalité l'accès au support informatique en charge de la création et de la réinitialisation des mots de passe.

Une conservation des données pendant une longue durée peut causer des dégâts considérables tant à l'aéroport qu'à chaque employé étant enrôlé dans la base de données si un piratage conduit à une fuite des données. L'Agence européenne pour la sécurité aérienne (EASA) estime que le premier challenge de l'aviation est la cyber sécurité. Afin de relever ce défi, on peut notamment utiliser ce qu'on appelle la « *Block Chain* ».

La « *Block Chain* » est une technologie de stockage et de transmission de données sans organe de contrôle. Les informations envoyées par les utilisateurs sont vérifiées et groupées à intervalle régulier en bloc, formant ainsi une chaine. Ces données sont bien évidemment cryptées et protégées contre toute falsification ou suppression. Actuellement la technologie est surtout utilisée pour les transactions en crypto-monnaies et autres activités à caractères financières.

III. L'exemple de l'EuroAirport Bâle-Mulhouse.

Durant 8 semaines, l'aéroport de Bâle Mulhouse a effectué des tests de reconnaissance faciale pour l'accès en ZSAR avec la société Gemalto. Puisqu'il s'agissait d'un test, la base de données établie pour l'expérimentation ne pouvait pas être mise à jour régulièrement et le consentement des personnes enrôlées étaient nécessaire, c'est pourquoi le test n'était pas obligatoire mais basé sur le volontarisme des employés.

Bien que des petites complications liées à l'installation de la caméra aient eu lieu au début, le test s'est globalement bien déroulé et la reconnaissance faciale a été grandement apprécié par le personnel et les agents de sûreté. La caméra a été très rapide dans la reconnaissance des visages puisqu'elle mettait en moyenne 2.81 secondes pour authentifier un visage. D'ailleurs les performances en reconnaissance faciale de la caméra utilisée permettent d'authentifier un employé une photo très ancienne enrôlée dans la base de données ou encore des modifications au visage (cicatrice, pilosité faciale ou port de lunettes de soleil).

L'utilisation de la reconnaissance faciale, comme tout autre méthode d'identification, présente un risque lié au détournement de finalité. En effet, la caméra qui a été installée dispose d'un angle d'observation assez large qui permet de voir et suivre le comportement de plusieurs individus en même temps. Ceci présente un risque pour les

agents de sûreté et autre personnes soucieux du respect de leur intimité en milieu de travail. Ce droit est reconnu par la jurisprudence, notamment celle de la Cour de cassation, qui estime que le salarié a le droit au respect de l'intimité de sa vie privé au lieu et heure de travail[82]. De ce fait, les juges effectuent un contrôle strict du respect de la finalité des outils biométriques déployés dans le cadre d'une entreprise.

[82] Arrêt n° 4164 du 2 octobre 2001 Cour de cassation - Chambre sociale

Chapitre 2 :
Le respect nécessaire de la finalité de l'utilisation de la reconnaissance faciale

La reconnaissance faciale est une technologie particulière car elle dispose d'une multi-finalité. Elle permet certes de reconnaître les individus et de les identifier, mais elle peut également servir au suivi des individus et au contrôle de leur comportement. C'est pourquoi la jurisprudence est très rigoureuse dans le respect de la finalité des outils biométriques (I), d'autant plus que l'utilisation d'une donnée biométrique réduit la barrière entre l'individu et son monde professionnel. (II).

I. Une jurisprudence rigoureuse dans le contrôle du respect de la finalité

Les activités de surveillance sont déléguées à des machines. Or, si l'employeur a le droit de surveiller l'activité de ses salariés pendant leur temps de travail, l'emploi de procédés clandestins de surveillance est illicite. Ainsi il doit porter à la connaissance du salarié tous les dispositifs qu'il utiliser pour la surveillance[83]. La jurisprudence se montre donc extrêmement rigoureuse en ce qui concerne les méthodes employées pour informer les salariés et veille scrupuleusement non seulement au respect des dispositions formelles, mais également au principe de loyauté. C'est pour cela qu'elle a notamment rejeté le moyen de preuve rapporter par la société EDF au motif que les cadres ayant surveillé un des salariés de l'entreprise n'avait ni décliné leur identité ni le motif de leur visite au à ce dernier[84].

Rappelons également que les traitements ayant pour finalité la gestion des horaires sont explicitement interdits. La CNIL a toujours refusé toute tentative de recours à la biométrie à ces fins. Elle estime qu'une raison de sécurité doit justifier un « recours impératif à la biométrie » pour autoriser de tels dispositifs. En effet dans sa délibération n° 2013-327 du 24 octobre 2013 elle refuse la mise en œuvre par la société SA DAMELIE d'un traitement de données à caractère personnel reposant sur un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle du temps de travail. Par analogie, on peut penser que l'utilisation de la reconnaissance faciale à ce but peut être sanctionnée par la CNIL, d'autant plus que

[83] Cour de Cassation, Chambre sociale, du 14 mars 2000, 98-42.090
[84] (Cour de cassation, Ch. Social, 18 mars 2008, n° 06-45093).

depuis l'entrée en vigueur de la RGPD les sanctions sont très lourdes avec une amende qui peut s'élever à 20 Millions d'euros ou dans le cas d'une entreprise à 4% du chiffre d'affaire annuel mondial[85]. De plus, l'activité litigieuse peut également être suspendue en cas de manquement au RGPD.

Enfin lorsqu'on met en place un système de reconnaissance faciale, on établit une relation tripartite entre le fournisseur, l'entreprise utilisatrice et l'employé utilisateur. Les informations sont accessibles par un tiers qui n'est pas identifiable par la personne soumise à la reconnaissance faciale, ce qui pose le problème de l'utilisation des données à des fins commerciales ou disciplinaires. C'est pourquoi il faut bien encadrer l'utilisation des données biométriques par un tiers.

II. L'effacement de la distinction entre monde du travail et vie privée du fait de l'utilisation de la reconnaissance faciale

Lorsqu'un employé donne une information relative à une identification, comme son badge, cela n'équivaut pas à donner une information biométrique comme son visage ou son empreinte digitale. Le premier n'a de sens que pour l'entreprise dans laquelle il travail, alors que l'identificateur biométrique c'est l'individu lui-même. De ce fait, la personne est mobilisée au pouvoir de l'entreprise et soumis au pouvoir hiérarchique en tant qu'individu et non en tant qu'employé. Ce terme « employé » réduit la subordination au cadre professionnelle, alors qu'avec la biométrie ce cadre s'efface et on domestique l'humain qui est instrumentalisé au profit de son activité professionnelle[86].

L'identité biométrique est un nouveau type d'identité qui se distingue des procédés classiques car elle peut être utilisée en dehors du contexte dans lequel l'application biométrique est programmée. C'est l'une des principales craintes de la CNIL et des associations civiles qui dénoncent le risque de voir une banalisation des interconnexions de fichiers susceptibles de favoriser la mise en place d'un « Big Brother administratif » permettant de tracer les individus dans les actes de leur vie courante.

[85] https://www.cnil.fr/fr/definition/sanction
[86] A. Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 8 : *L'identification biométrique dans l'entreprise* par G.Deharo, §18

Parallèlement aux aéroports, deux établissements scolaires de Nice et de Marseille veulent utiliser la reconnaissance faciale pour contrecarrer le manque d'effectif des surveillants. Pour ce faire, des élèves volontaires ont reçu un badge avec leurs informations biométriques. Avant d'entrée dans l'établissement, ils doivent passer par des portiques où une caméra analyse leur visage et envoie les informations au bureau des surveillants : un cadre vert s'affiche si l'élève fait partie de l'établissement, un cadre jaune s'affiche s'il s'agit d'un visiteur qui n'a pas de badge et enfin un cadre rouge apparaît si l'élève tente de dissimuler son badge ou s'il ne correspond pas au badge. La CNIL a suivi de très près cette expérimentation qui soulève beaucoup de question notamment par rapport à la finalité de ce type de pratique. En effet, le risque de détournement n'est pas négligeable, puisque grâce à ce dispositif on peut connaître les heures d'arrivée de chaque étudiant, observer leur comportement et peut être même les sanctionner avec les images qui sont fournies par la caméra.

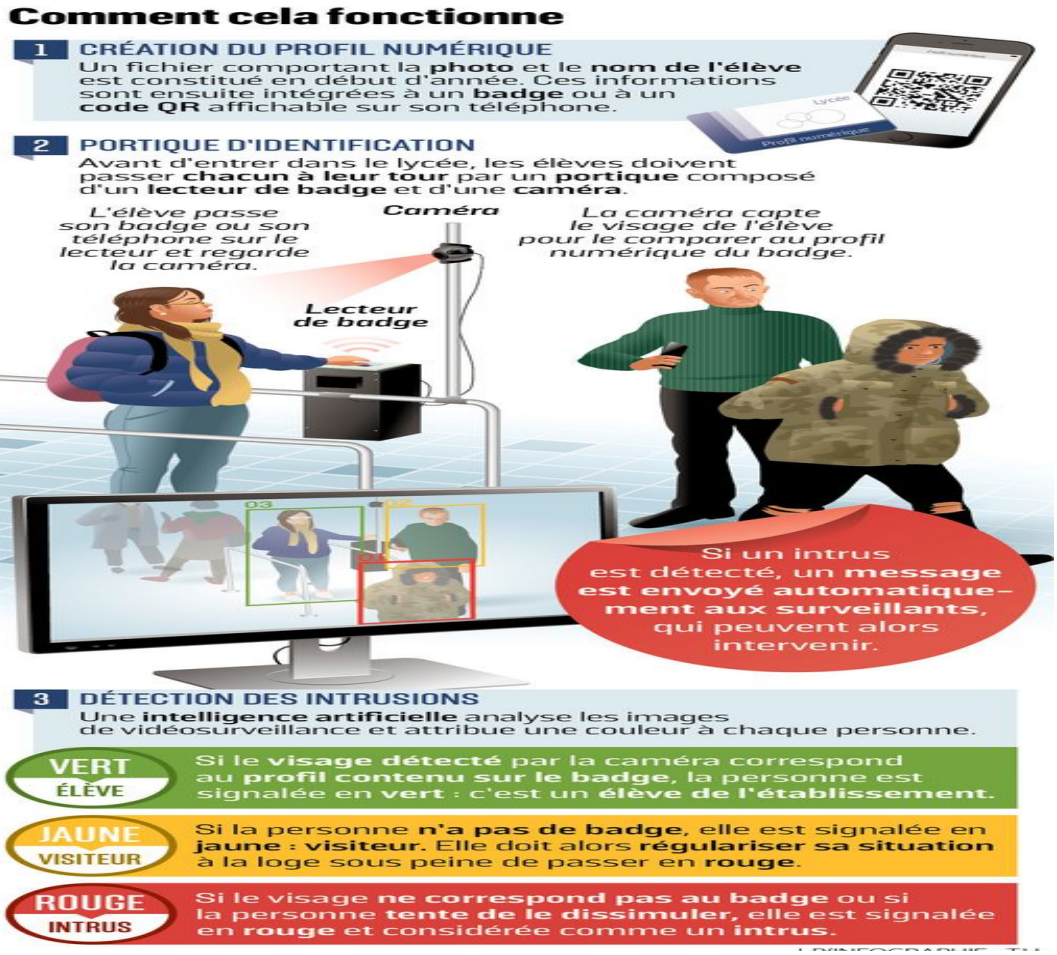

Figure 9: Fonctionnement de la reconnaissance faciale dans les deux lycées de la région PACA - Source : http://www.leparisien.fr/societe/video-dans-les-lycees-et-maintenant-place-a-la-reconnaissance-faciale-

Conclusion sur la deuxième partie :

Les aéroports font de plus en plus usage de la reconnaissance faciale pour à la fois faciliter l'expérience passager et gérer les accès sur le site. Le premier cas de figure remet en question des pratiques et coutumes bien implantées, comme le fait d'avoir un passeport. En effet, le passeport est synonyme de la citoyenneté et le reflet de la souveraineté de l'Etat qui nous le fournit. Néanmoins, les technologies actuelles rendent ce document de plus en plus obsolète et c'est d'ailleurs pour ça que l'IATA invite les Etats à prendre des initiatives pour remplacer le passeport.

De l'autre côté, les aéroports font face à des problèmes d'infrastructures. Contrainte par la géographie de leur territoire et des règlementations, ils ne peuvent pas s'étendre sans limite. C'est pour cela qu'ils décident de recourir à des technologies d'identification plus rapide comme la reconnaissance faciale afin de mieux gérer le flux de passager croissant, mais aussi les accès dans les zones réservées. Les nécessités en terme de FAR ne sont pas les mêmes pour les accès, mais il convient de préciser que la faiblesse de la reconnaissance faciale réside dans les doubles biométriques. En effet, il est presque impossible pour une caméra de faire la distinction entre des jumeaux.

Conclusion générale

Aujourd'hui l'identification surpasse la relation de l'Etat avec son citoyen. Des acteurs internationaux, comme l'OACI ou les institutions européennes, jouent eux aussi un rôle prépondérant. Le marché aussi a son mot à dire puisque les industriels développent des relations avec les gouvernements et les entités de standardisations.

Toutefois, la décision de recourir à la biométrie repose sur des logiques qui vont au-delà d'une rationalité économique. Elle est essentiellement politique en ce sens qu'elle vise à créer au sein de la population le sentiment d'être protégé par l'Etat et ses agences de sécurité dans un contexte d'incertitudes. Ce sentiment contribue fortement à réaffirmer la fonction wébérienne de la politique, celui du monopole de la violence légitime détenu par l'Etat, que les attentats du 11 septembre 2001 avaient défié et effrité[87]. Ce qui a commencé comme une guerre contre le terrorisme a été bascule vers un nouvel agenda sécuritaire et ce qui a commencé par donner du pouvoir aux agences gouvernementales pour combattre le terrorisme a donné plus de pouvoir au gouvernement de manière générale.

C'est exactement ce que les opposants à cette technologie invoquent comme argument. Ils craignent le détournement de finalité qui conduirait ainsi les individus à vivre dans une « *société de contrôle* ». Cette expression développée par les philosophes Gilles Deleuze et Antonio Negri s'inspire de la pensée de Michel Foucault. Ainsi ce type d'organisation de la société, qui s'appuie sur l'évolution technique et le développement des technologies de l'information et de la communication, semble garantir une plus grande marge de manœuvre aux individus et davantage de mobilité. Contrairement aux dispositifs disciplinaires classiques qui procèdent par la coercition, aujourd'hui le mouvement et la liberté de circulation sont les conditions nécessaires à l'exercice d'un pouvoir qui opère désormais par *« contrôle continu »* de tous les aspects de l'existence et par *« communication instantanée »*.

On remarque à l'heure actuelle une dichotomie qui devrait être dépassée, Bruce Schneir disait que « *la sécurité n'est pas liée à la technologie, elle est liée aux risques*

[87] A.Ceyhan, *L'identification biométrique : Champs, acteurs, enjeux et controverses* - Chapitre 20, *« Acceptabilité » de la biométrie : linéaments d'un cadre analytique*

et aux mangements du risque. Les bons systèmes de sécurité impliquent le travail conjoint de la technologie et de l'humain, mais ce sont ces derniers qui doivent mener la technologie et non l'inverse [88]».

Il est donc nécessaire d'aller au-delà des divisions classiques en matière de reconnaissance faciale qui d'une part estime que cette technologie rend la société plus confortable et d'autre part menace nos libertés car son infaillibilité n'est qu'un mythe. Aujourd'hui les systèmes de reconnaissance faciale sont suffisamment performants pour assurer une authentification lors du passage aux frontières ou pour les contrôle d'accès. Il faut voir ces systèmes comme un ensemble qui comprend à la fois la caméra, mais aussi le facteur humain derrière. Tant qu'un cadre juridique permettant d'équilibrer l'utilisation des outils de reconnaissance faciale sera présent, cette technologie permettra des avancées inégalées en terme de sécurité au sein de nos sociétés.

[88] B. Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (New York: Copernicus, **2003),** 146.

Bibliographie

I. Livres

A.Ceyhan et P.Piazza, « L'identification biométrique : champ, acteurs, enjeux et controverses », 16 juin 2011,

D. McCormack, « Can Corporate America secure our nation ? An analysis of the Identix Framework for the regulation and use of face recognition technology », 2003

K. A. Gates, « Our Biometric Future : Facial Recognition Technology and the culture of surveillance », 2011

Noémie Véron, « Le contrôle de l'utilisation des données biométriques au regard du droit au respect de la vie privée », *l'Harmattan*, 2017

B. McPhail, C. Parsons, K.L. Smith, J. Ferenbok & A.Clement, « Identifying Canadians at the Border : ePassports and the 9/11 legacy », 2012

II. Thèses et mémoires

G. Dominique, Y. Fan and P. Michel, « Design, Implementation and Evaluation of Hardware Vision Systems dedicated to Real-Time Face Recognition », 2007

Y. Welinder, « A face tells more than a thousand posts: developing face recognition privacy in social networks », 2012

Z. Wu & R. J. Radke, « Real-Time Airport Security Checkpoint Surveillance Using a Camera Network », Juin 2011

J. Hatin, « Evaluation de la confiance dans un processus d'authentification », 2018

Dr. M. Hasanuzzaman & Dr. H. Ueno, « Face and Gesture Recognition for Human-Robot Interaction », 2007

A. Khashman, « Intelligent Global Face Recognition », 2007

T. Papatheodorou & D. Rueckert, « *3D Face Recognition* », 2007

A. Pnevmatikakis and L. Polymenakos, « Far-Field, Multi-Camera, Video-to-Video Face Recognition », 2007

L. Ballihi, B. Ben Amor, M. Daoudi, A. Srivastava & D. Aboutajdine, « Sélection de caractéristiques géométriques pour la reconnaissance faciale 3D », 2013

N. Köse, « Spoofing and Disguise Variations in Face Recognition », 2016

R. Auguste, « Reconnaissance dynamique des personnes dans les émissions audiovisuelles », 2015

III. Convention internationales et normes européennes

Convention de Chicago du 7 décembre 1944

Annexe 9 – Facilitation

Annexe 17 – Sûreté

Règlement général sur la protection des données (règlement n° 2016/679)

Traité d'Amsterdam du 2 octobre 1997

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981

Article 8 de la Convention européenne de droits de l'Homme

Directive du 24 octobre 1995 (95/46/CE)

Directive relative aux données des dossiers passagers le 21 avril 2016

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

Règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile

IV. Jurisprudences

CEDH, S. et Marper c. Royaume Uni, 4 décembre 2008

CJUE, Michael Schwarz c. Stadt Bochum, 17 octobre 2013

CJUE, 4ème chambre, arrêt du 16 avril 2015

US Supreme Court, Katz v. United States, 18 decembre 1967

US Supreme Court, Kyllo v. United States, 11 juin 2001

US Supreme Court, Dow Chemical Co v. United States, 19 mai 1986

Conseil Constitutionnel, Décision n° 2012-652 DC, 22 mars 2012

Conseil d'Etat, Association pour la promotion d'image et autre, 26 octobre 2011

V. Articles

B. J. Muller, « (Dis)Qualified Bodies: Securitisation, Citizenship and 'Identity Management »

I. Lelieur & C. Vernudachi, « Le RGPD, un an après son entrée en vigueur, quels enjeux pour les aéroports ? » 2019

P. E. Agre, « Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places », 10 septembre 2003

F. Maurin, « Through new solutions, IDEMIA offers biometry for all », International Airport Review, 16 juilet 2019

B. S. Swann & J. Loudermilk, « Facial recognition: A strategic imperative for national security », Biometric Update, 3 juin 2019

C. Burt « IATA unanimously resolves to speed adoption of One ID for biometric air travel », 3 juin 2019

C. Burt « San Francisco passes ban on police and city use of public facial biometrics » Biometric Update, 15 mai 2019

C. Burt « Biometrics Institute warns biometrics misuse could undermine public confidence », Biometric Update, 22 mai 2019

J. Reid « Airport facial recognition: What you need to know », Business traveller, 9 juin 2019

J. Reid « Facial recognition kiosk gives flight updates at Chinese airport », Business traveller, 27 mars 2019

J. Reid « Lufthansa launches biometric boarding at Miami International Airport », Business traveller, 5 février 2019

J. Reid « Cathay Pacific begins biometric boarding trial at AMS », Business traveller, 19 février 2019

J. Reid « Hamad International rools out ent to end facial recognition », Business traveller, 29 mai 2019

C. Bright, « Tokyo Narita Airport to introduce end-to-end facial recognition in 2020 », Business traveller, 22 mars 2019

Airport technology, « Amadeus pilots biometric boarding technology at Ljubljana Airport », 17 mai 2019

International Airport Review, « IDEMIA reveals the know-how behind the rise of multi-modal biometrics », Mars 2019

T. Lozier, « In the Age of facial recogntion, the Human element is still necessary », Security Magazine, 29 mai 2019

D. Higgins, « The rise of biometric authentication », techradar, 29 mai 2019

Planet Biometrics, « Integrated Biometrics sensor protects US cargo facility », Mai 2019

M. Miller, « Congress raises privacy concerns with airport security pictures », 4 juin 2019

Arabian Aerospace, « How technology is making aviation safer », 14 juin 2019

A. Gailey, « Delta to launch facial recognition technology in more U.S. airports, CEO Ed Bastian says », bizjournals, 17 juin 2019

D. B. Johnson, « DHS building consolidated system for biometric data », 24 juin 2019

E. Wang, « Biometrics: The safest and fastest means of identification », International Airport Review, 25 juin 2019

K. Lightman, « How automation could make airports more efficient », 26 juin 2019

S. R. Kelleher, « Paradigm Shift: Biometrics And The Blockchain Will Replace Paper Passports Sooner Than You Think », Forbes, 28 juin 2019

E. Birnbaum, « Government privacy watchdog to probe airport facial recognition », The Hill, 28 juin 2019

D. Nyczepir « Biometrics are pushed to improve as DHS, NIST continue to test algorithms », Fedscoop, 28 juin 2019

J. Bachman, « The struggle to turn your face into secure travel ID », Bloomberg, 1 juillet 2019

M. Jaikrishna, « Air travel needs cybersecurity, now tighter than ever », Financial Express, 2 juillet 2019

M. Scott, « Europe eyes stricter rules on facial recognition », politico.eu, 2 juillet 2019

Lee KAIR, « Biometrics can protect our borders – along with our privacy », The Hill 9 juillet 2019

International Airport Review, « JFK and Vision-Box roll out facial recognition boarding », 13 mai 2019

L. Dormehl, « How facial recognition is changing life as we know it – for better or worse », 13 mai 2019

T. Rebner, « Behavioral biometrics is the future of user authentication », Forbes, 13 mai 2019.

E. White, « The future looks bright for facial recognition devices », Federal news network, 15 mai 2019

Planet Biometrics, « EU Council adopts biometric justice regulations », 15 mai 2019

A. Sable, « Biometric technology industry: Trend of innovation arrives, implementation for national security gains importance », 17 mai 2019

C. Lo, « A first in rail : Eurotunnel rolls out facial recognition tech », Railway Technology, 21 mai 2019

Emily Birnbaum, « DHS officials set for grilling over facial recognition technology », The Hill, 22 mai 2019

Manon Briquet, « Biométrie et vie privée »

VI. Rapports publics

L. D. Introna & H. Nissenbaum, « Face recognition Technology : a survey of policity and implementation issues », Juillet 2009

Center for Democracy and Technology (CDT), « Facial Recognition & Privacy : An EU-US perspective », 8 octobre 2012

International Airport Review, « GUIDE TO… Biometrics: Seamless-travel instigator or cyber-security worry? », 2019

Assises nationales du transport aérien, « Rapport des travaux : Performance et innovation au service des passagers »

VII. Sites internet

IATA : www.iata.org

OACI : www.icao.int

CNIL : www.cnil.fr

British Airways : www.britishairways.com

IDEMIA : www.idemia.com

Gemalto : www.gemalto.com

Aéroport de Londres-Heathrow : www.heathrow.com

Assises nationales du transport aérien : https://www.assisesdutransportaerien.gouv.fr

Table des matières