N° 788

SÉNAT

SESSION EXTRAORDINAIRE DE 2015-2016

Enregistré à la Présidence du Sénat le 13 juillet 2016

RAPPORT D´INFORMATION

FAIT

*au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur l'***usage** *de la* **biométrie** *en* **France** *et en* **Europe***,*

Par MM. François BONHOMME et Jean-Yves LECONTE,

Sénateurs.

(1) Cette commission est composée de : M. Philippe Bas*, président ;* Mme Catherine Troendlé, MM. Jean-Pierre Sueur, François Pillet, Alain Richard, François-Noël Buffet, Alain Anziani, Yves Détraigne, Mme Éliane Assassi, M. Pierre-Yves Collombat, Mme Esther Benbassa*, vice-présidents ;* MM. André Reichardt, Michel Delebarre, Christophe-André Frassa, Thani Mohamed Soilihi*, secrétaires ;* MM. Christophe Béchu, Jacques Bigot, François Bonhomme, Luc Carvounas, Gérard Collomb, Mme Cécile Cukierman, M. Mathieu Darnaud, Mme Jacky Deromedi, M. Félix Desplan, Mme Catherine Di Folco, MM. Christian Favier, Pierre Frogier, Mme Jacqueline Gourault, M. François Grosdidier, Mme Sophie Joissains, MM. Philippe Kaltenbach, Jean-Yves Leconte, Roger Madec, Alain Marc, Didier Marie, Patrick Masclet, Jean Louis Masson, Mme Marie Mercier, MM. Michel Mercier, Jacques Mézard, Hugues Portelli, Bernard Saugey, Simon Sutour, Mmes Catherine Tasca, Lana Tetuanui, MM. René Vandierendonck, Alain Vasselle, Jean-Pierre Vial, François Zocchetto.

S O M M A I R E

Pages

LISTE DES PROPOSITIONS

Proposition n° 1 : Poursuivre le développement de l'identité numérique utilisant des données biométriques (ALICEM), comme envisagé par l'ANTS, en valider la fiabilité et travailler à son indispensable encadrement juridique. Coordonner cette démarche avec les autres initiatives européennes.

Proposition n° 2 : Pour permettre à l'État de garder l'initiative en matière d'identification et lutter contre les usurpations d'identité, créer une carte nationale d'identité biométrique, conformément à la logique de la loi n° 2012-410 du 27 mars 2012, et présentant les caractéristiques suivantes :

- conservation de deux empreintes digitales ;

- lien avec un fichier comprenant des « liens faibles » ;

- exclusion des usages commerciaux et notamment des possibilités d'achats en ligne.

Proposition n° 3 : Recueillir les données biométriques des nouveaux titulaires de certificat de nationalité française (CNF), lors de leur délivrance, et introduire ces données dans le fichier des passeports pour lutter contre la fraude documentaire.

Proposition n° 4 : Poursuivre la modernisation des procédures de délivrance des passeports et des visas biométriques :

- mettre en œuvre l'envoi sécurisé des passeports des Français de l'étranger prévu par le décret n° 2015-701 du 19 juin 2015 ;

- éviter un nouveau recueil d'empreintes lors d'un renouvellement de passeport biométrique ;

- approfondir la politique de mutualisation de la collecte des données biométriques des visas et l'étendre aux passeports ;

- harmoniser au niveau européen les collectes de données biométriques incluses dans les passeports européens et pour les visas ;

- mener à son terme l'expérimentation de recueil mobile de ces données.

Proposition n° 5 : Relancer la procédure d'échange de certificats de sécurité entre les États membres de l'espace Schengen pour permettre à chacun d'eux d'accéder aux empreintes digitales enregistrées dans les passeports et les titres de voyage biométriques émis par des pays de l'espace Schengen.

Proposition n° 6 : Offrir au niveau européen des garanties au moins identiques à celle données par la CNIL en France dès lors qu'il apparait indispensable d'harmoniser nos dispositifs de recueil de données dans les fichiers européens et de croiser certains de nos fichiers nationaux.

Veiller à ce que chaque développement et croisement de fichiers envisagé s'effectue dans un environnement respectant strictement la finalité des fichiers utilisés et le principe de proportionnalité.

Proposition n° 7 : Étendre le système d'entrée/sortie (EES) aux frontières de l'espace Schengen aux ressortissants communautaires, sans constitution, sauf situation spécifique, motivée et encadrée, d'historique des mouvements constatés.

Proposition n° 8 : Accepter une expérimentation de la reconnaissance faciale reliant les systèmes de vidéoprotection à des fichiers de « personnes à risque », l'objectif étant de disposer de nouveaux outils pour prévenir et réprimer les actes terroristes dans des conditions de forte affluence qui limitent, et parfois rendent même dangereux, le recours à des fouilles ou à des contrôles systématiques.

Prévoir des garanties spécifiques, notamment en :

- s'inspirant, en plus restrictif, des modalités de conservation des données du système de lecture automatisée des plaques d'immatriculation (LAPI) ;

- prévoyant une durée d'expérimentation limitée à un an.

Proposition n° 9 : Tout en ne perdant pas de vue que la biométrie n'est pas infaillible et qu'il convient d'en comprendre les limites, disposer de conditions économiques et juridiques permettant de préserver et renforcer les capacités de françaises de recherche et développement afin de conserver la maîtrise de l'élément de souveraineté que représentent les outils biométriques.

Mesdames, Messieurs,

Votre commission a souhaité confier à MM. François Bonhomme et Jean-Yves Leconte une mission d'information visant à dresser un panorama des usages de la biométrie et à évaluer les perspectives d'évolution envisageables.

Comme le soulignait notre ancien collègue député, M. Christian Cabal, *« quasiment tout dans l'anatomie ou le comportement d'un individu peut être transformé en un code informatique permettant de l'identifier »*[1].

La biométrie désigne **l'ensemble des technologies de reconnaissance physique ou biologique des individus**. D'abord centrées sur les empreintes digitales et génétiques, les techniques biométriques se sont diversifiées : la reconnaissance faciale, l'examen de l'iris, l'analyse de la pression sanguine, de la forme de l'oreille, *etc.* constituent aujourd'hui des moyens d'authentification et d'identification déjà opérationnels ou en cours de développement.

Les usages privés de la biométrie ont été analysés par votre commission à l'occasion de l'examen de la proposition de loi n° 361 (2013-2014) de M. Gaëtan Gorce. Le rapporteur, M. François Pillet, avait alors constaté la banalisation de ces techniques[2]. Au terme d'un débat nourri, le Sénat avait conclu à la nécessité de réserver ces utilisations dans le domaine privé à des usages sensibles dont la finalité comprend, par exemple, la protection de l'intégrité physique des personnes ou la protection d'informations dont la divulgation, le détournement ou la destruction représenterait un préjudice grave et irréversible.

---

[1] « Les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques mises en œuvre », *rapport n° 355 (2002-2003) fait au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, p. 14* (*http://www.senat.fr/notice-rapport/2002/i0938-notice.html*).

[2] *Rapport n° 465 (2013-2014), fait au nom de la commission des lois du Sénat* (*http://www.senat.fr/rap/l13-465/l13-4651.pdf*).

Le présent rapport aborde la biométrie sous un angle différent : celui des usages publics. Il s'agit d'analyser la façon dont l'administration utilise ces techniques à des fins judiciaires mais également administratives et de prévention (police administrative, simplification des relations entre le citoyens et l'administration).

Vos rapporteurs se sont ainsi interrogés sur les évolutions technologiques en cours et sur la manière dont elles pourraient améliorer l'efficacité de l'action administrative tout en respectant le droit à la vie privée des personnes.

I. LES USAGES PUBLICS DE LA BIOMÉTRIE SE SONT PROGRESSIVEMENT DÉVELOPPÉS DANS UN CADRE JURIDIQUE SPÉCIFIQUE

D'abord réservé au domaine judiciaire, l'usage de la biométrie a été progressivement étendu à la sphère administrative, notamment sous l'influence du droit communautaire et des préoccupations de prévention d'actes terroristes. Ainsi, après les attentats du 11 septembre 2001, les États-Unis ont imposé un passeport biométrique pour entrer sur le sol américain sans visa, ce qui a conduit à l'établissement des règles européennes en vigueur.

Pour l'autorité publique, l'objectif de ces techniques est double : sécuriser l'authentification et l'identification des personnes, d'une part, et rendre l'action administrative plus efficace, d'autre part.

Les données biométriques sont strictement encadrées par des **principes de proportionnalité et de finalité** définis par le droit européen et national.

A. LE DÉVELOPPEMENT ET LA DIVERSIFICATION DES TECHNIQUES BIOMÉTRIQUES

Le marché mondial de la biométrie connaît une expansion certaine alors que ce type de technologies fait aujourd'hui partie intégrante des procédures administratives.

D'après l'agence *Acuity market intelligence*[1], ce marché représenterait **près de 9 milliards d'euros** partagés à parité entre les usages publics et les usages privés.

L'industrie française compte dans ses rangs des leaders mondiaux comme *Safran identity and security* (ex *Morpho*), *Gemalto* ou *Thalès*.

[1] *Étude disponible à l'adresse suivante : http://www.acuity-mi.com/FOB_Report.php.*

L'activité des entreprises françaises de biométrie : quelques exemples emblématiques

Safran identity and security fournit par exemple les sas PARAFE ou les cartes nationales d'identité égyptiennes et participe au programme d'identification biométrique de la population indienne. Entendus par vos rapporteurs, ses représentants ont évalué le chiffre d'affaires de leurs solutions biométriques à 1,3 milliards d'euros, l'entreprise employant 8 000 collaborateurs dont 1 500 en France.

Gemalto a participé au programme «*identification biométrique officielle au Gabon* » (IBOGA) ou à la constitution d'un registre électoral biométrique au Burkina Faso. La société fournit, en outre, la technologie utilisée par les passeports de nombreux États comme la Belgique, Malte ou l'Algérie.

Thalès revendique l'émission de plus de 300 millions de titres d'identité. L'entreprise a participé à la création de l'application de gestion des dossiers des ressortissants étrangers en France (AGDREF 2) ainsi qu'au programme d'externalisation du recueil des données biométriques des visas (BIONET). Elle a également fournit les cartes nationales d'identité du Kenya ou du Cameroun.

Historiquement, les dispositifs biométriques utilisaient essentiellement les empreintes digitales et génétiques, techniques qui demeurent les plus fiables à ce jour.

Prélèvement d'une empreinte digitale (capteur PARAFE)

Source : Direction centrale de la police aux frontières (DCPAF)

Deux dynamiques sont aujourd'hui constatées sur le marché de la biométrie :

- de **nouvelles techniques de reconnaissance anatomique** apparaissent avec des degrés de fiabilité divers (géométrie de la main, voix, odeur, forme de l'oreille, pression sanguine, *etc.*), les outils de **reconnaissance faciale** et de **contrôle de l'iris**[1] connaissant l'expansion la plus rapide ;

[1] Cf. *la seconde partie du présent rapport pour l'utilisation des outils de reconnaissance faciale et de contrôle de l'iris dans le cadre du programme* « frontières intelligentes ».

- **des dispositifs de reconnaissance dynamique** sont en phase de développement. Il s'agit, à titre d'exemple, d'utiliser des logiciels d'analyse comportementale reliés aux caméras de vidéoprotection et de détecter les risques potentiels en mesurant les différentiels de température du corps des individus, le niveau de leur voix, *etc*. Un tel dispositif est expérimenté dans le domaine ferroviaire comme la mission d'information sur la sécurité dans les gares a pu le constater début 2016[1].

1. Un recours croissant aux outils biométriques

a) Un premier usage dans le domaine judiciaire

Historiquement, **la biométrie a d'abord été utilisée dans le cadre de procédures criminelles** pour faciliter l'identification des auteurs d'infractions et l'instruction des affaires.

En 1879, le criminologue **Alphonse Bertillon**, alors employé de la Préfecture de police de Paris, crée une méthode d'identification, le « *bertillonnage* », consistant à prendre les photographies et huit mensurations de prisonniers afin de les identifier plus facilement en cas de récidive. Entre 1883 et 1884, 19 771 individus sont ainsi mesurés et 290 d'entre-eux sont identifiés lors d'enquêtes ultérieures[2].

Ces modes d'identification par mesures biométriques furent **aussi à l'origine de dérives**, comme le carnet anthropométrique imposé aux gens du voyage par la loi du 16 juillet 1912[3] ou au cours de la seconde guerre mondiale. C'est pourquoi ces méthodes, couplées à la puissance de calcul des dispositifs informatiques d'aujourd'hui, représentent un risque majeur pour les libertés et méritent une attention particulière ainsi qu'un encadrement spécifique.

---

[1] « Renforcer la sécurité des transports terrestres face à la menace terroriste », *rapport n° 291 (2015-2016) de MM. Alain Fouché et François Bonhomme, p. 44-45 (http://www.senat.fr/rap/r15-291/r15-2911.pdf).*

[2] *Source :* « Alphonse Bertillon et l'anthropométrie judiciaire. L'identification au cœur de l'ordre républicain », *Martine Kaluszynski, Revue criminocorpus, mai 2014 (http://criminocorpus.revues.org/2716 ; DOI : 10.4000/criminocorpus.2716).*

[3] *Loi relative à l'exercice des professions ambulantes.*

Une fiche anthropométrique d'Alphonse Bertillon (1912)

Source : « Alphonse Bertillon
et l'anthropométrie judiciaire.
L'identification au cœur de l'ordre républicain »,
Martine Kaluszynski, Revue criminocorpus, mai 2014

Les enquêtes criminelles s'appuient principalement sur **deux fichiers** : le premier porte sur les empreintes digitales (**fichier automatisé des empreintes digitales**, FAED), le second sur les empreintes ADN (**fichier national automatisé des empreintes génétiques**, FNAEG).

Ces bases de données sont administrées par la direction centrale de la police judiciaire du ministère de l'intérieur, sous le contrôle des magistrats de l'ordre judiciaire.

Le FAED et le FNAEG sont utilisés dans un cadre précisément défini par les lois et règlements par des fonctionnaires de police et de gendarmerie spécialement habilités. En **2014**, le **FAED** a par exemple permis d'identifier des individus dans le cadre de **14 698 affaires**[1].

[1] *Rapport d'information n° 2778 sur la prescription en matière pénale de MM. Alain Tourret et Georges Fenech fait au nom de la commission des lois de l'Assemblée nationale, mai 2015, p. 390 (http://www.assemblee-nationale.fr/14/rap-info/i2778.asp).*

Les conditions d'utilisation du FAED

Les conditions d'utilisation du fichier automatisé des empreintes digitales (FAED) sont définies dans le **décret n°87-249 du 8 avril 1987**[1], ce dernier précisant notamment les éléments enregistrés ainsi que les conditions de consultation et de gestion du fichier.

- Les éléments enregistrés

Les empreintes du FAED sont **enregistrées dans un cadre judiciaire** lors d'une enquête pour crime ou délit flagrant, d'une enquête préliminaire, d'une commission rogatoire, d'une information pour recherche des causes de la mort ou d'une disparition, d'une enquête consécutive à la découverte d'une personne grièvement blessée ou lors de l'exécution d'un ordre de recherche délivré par une autorité judiciaire.

Les empreintes sont insérées dans une fiche signalétique comprenant, en outre, des informations relatives à l'identité de la personne concernée (nom, prénoms, *etc.*), le service ayant procédé à la signalisation, la référence de la procédure et, le cas échéant, des clichés anthropométriques.

- Les conditions de consultation

Environ **300 fonctionnaires de police et de gendarmerie** disposent d'un accès individuel au FAED. Ils peuvent uniquement le consulter dans le cadre d'opérations d'identification prévues par le décret précité (demande de l'autorité judiciaire ou des forces de l'ordre lors d'une enquête judiciaire, identification de personnes décédées, *etc.*). Le recours au FAED ***« hors du cadre judiciaire »*** **–** pour que le maire puisse s'assurer de l'identité d'une personne avant la fermeture du cercueil par exemple **–** **demeure l'exception**.

- La gestion du fichier

Les données du FAED sont **conservées pendant 25 ans** sauf si elles deviennent obsolètes (décision de relaxe ou d'acquittement devenue définitive par exemple) ou si la personne concernée obtient leur effacement dans le cadre des procédures de droit d'accès et de rectification prévues par la loi n° 78-17 du 6 janvier 1978[2].

Le champ couvert par le fichier automatisé des empreintes digitales et le fichier national automatisé des empreintes génétiques s'est progressivement étendu depuis leur création en 1987 pour le premier[3] et en 1998 pour le second[4].

Le FAED comprend les empreintes digitales de 5 millions de personnes tandis que le FNAEG contient les profils génétiques de 2,6 millions d'individus.

[1] *Décret relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur.*
[2] *Loi relative à l'informatique, aux fichiers et aux libertés.*
[3] *Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur.*
[4] *Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.*

Chacun de ces deux fichiers comporte, en outre, plus de 230 000 traces digitales ou génétiques non identifiées[1].

Ces données sont conservées pendant une durée maximale de 25 ans pour le FAED *(Cf. supra)* et de 40 ans pour le FNAEG.

L'extension du champ du FNAEG

Le fichier national automatisé des empreintes génétiques a été créé par la loi n° 98-468 du 17 juin 1998 pour identifier les auteurs de crimes et de délits à caractère sexuel.

Entre 2001 et 2007, six lois ont étendu son champ en incluant d'autres crimes et délits comme les atteintes volontaires à la vie de la personne, les actes de terrorisme[2], le trafic de stupéfiants, le proxénétisme[3], *etc.*

Les motifs permettant l'inclusion d'une empreinte génétique dans le FNAEG sont aujourd'hui précisés à **l'article 706-55 du code de procédure pénale**. Ils concernent les **personnes reconnues coupables** des infractions précitées mais **également celles dont « *il existe des indices graves ou concordants rendant (leur culpabilité) vraisemblable* »**.

Le FNAEG comprend, enfin, le génotype des cadavres non identifiés et des proches d'une personne disparue afin de faciliter les recherches.

b) L'essor des usages administratifs de la biométrie

Depuis le milieu des années 2000, un usage administratif des techniques biométriques s'est ajouté à cet usage judiciaire.

Ce mouvement a largement été influencé par le droit international et communautaire. Le passeport biométrique – créé en France en 2008[4] – correspond, à titre d'exemple, à l'application d'un règlement communautaire[5] lui-même inspiré de la préconisation de l'Organisation de l'aviation civile internationale (OACI) d'intégrer au moins une donnée biométrique dans les documents de voyage. Rappelons également, d'un point de vue pratique, que les États-Unis conditionnent depuis le 26 octobre 2006 leurs exemptions de visas à la présentation d'un passeport biométrique.

---

[1] *Source : rapport n° 386 (2014-2015) de Mme Joëlle Garriaud-Maylam, fait au nom de la commission des affaires étrangères du Sénat sur le projet de loi autorisant l'approbation de l'accord entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique relatif au renforcement de la coopération en matière d'enquêtes judiciaires, p. 12 (http://www.senat.fr/rap/l14-386/l14-3861.pdf).*

[2] *Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.*

[3] *Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.*

[4] *Décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.*

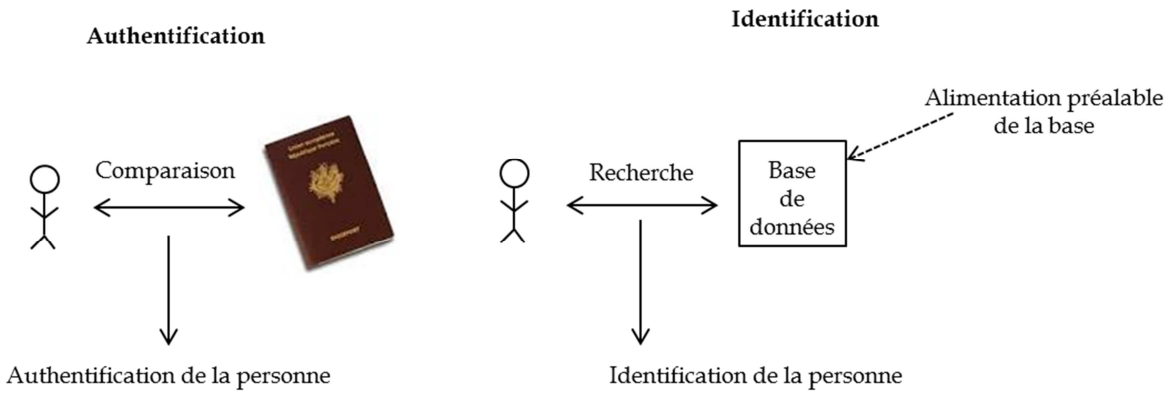
[5] *Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, modifié par le règlement (CE) n° 444/2009 du 28 mai 2009.*

Les techniques biométriques sont ainsi utilisées pour :

- **authentifier des personnes, c'est-à-dire vérifier l'exactitude de l'identité qu'elles allèguent.** Leurs données biométriques sont alors prélevées et comparées à celles figurant sur leur titre d'identité ;

- **identifier ces personnes, c'est-à-dire déterminer leur identité uniquement à partir de leurs données biométriques**. Ces données sont alors comparées avec celles contenues dans une base informatique associant, à titre d'exemple, des empreintes digitales déjà prélevées et les identités correspondantes.

La distinction entre authentification et identification



Source : commission des lois du Sénat

- ***L'authentification et l'identification des ressortissants français***

Les techniques biométriques servent, tout d'abord, à l'authentification et à l'identification à partir d'un **passeport biométrique** des ressortissants français voyageant à l'étranger[1].

Valable dix ans, ce document comporte une puce dans laquelle sont insérées les empreintes de la personne concernée ainsi que ses données d'état civil et son adresse.

L'ensemble de ces données est **conservé pendant quinze ans** dans le **fichier central de « *titres électroniques sécurisées* »[2] *(TES)*** dont la gestion relève du ministère de l'intérieur. La **finalité** de ce fichier est, d'une part, de

[1] *Dans les pays étrangers qu'ils visitent, les ressortissants français sont également astreints aux règles applicables aux visas de leur pays hôte (*Cf. *infra).*

[2] *Ce fichier comprend l'ensemble des huit empreintes recueillies alors que la puce du passeport biométrique n'en contient que deux.*

« ***mettre en œuvre la procédure de délivrance*** *(…) et de retrait des passeports* » et, d'autre part, de « ***détecter leur falsification et leur contrefaçon*** »[1].

Si les passeports biométriques sont formellement établis par les préfectures et sous-préfectures, les **données nécessaires à leur délivrance sont recueillies en mairie et dans les consulats** auprès d'agents individuellement désignés et spécialement habilités. **3 527 stations** sont déployées dans 2 088 communes et une dotation spécifique de 5 030 euros par an et par appareil est prévue pour indemniser les municipalités volontaires[2]. En outre, il est rappelé que la délivrance des passeports n'est pas liée au lieu de résidence du demandeur : il est tout à fait possible de solliciter sa délivrance dans une autre mairie ou un autre consulat.

Les passeports biométriques font aujourd'hui partis du quotidien des Français : **22,6 millions de passeports ont été produits entre juin 2009 et avril 2016** et près de 315 000 sont délivrés chaque mois[3].

- ***L'authentification et l'identification des ressortissants étrangers***

La biométrie est également utilisée pour **authentifier et identifier les ressortissants étrangers** à partir de trois principaux dispositifs : **les visas, le système EURODAC et l'application de gestion des dossiers des ressortissants étrangers en France (AGDREF 2).**

Les finalités de ces dispositifs regroupent des objectifs comparables à ceux de la base « *passeports* » (facilitation de la procédure administrative et lutte contre la fraude) auxquels s'ajoute l'objectif de « *lutter contre l'entrée et le séjour irréguliers des étrangers en France* »[4].

Les autorités diplomatiques et consulaires françaises délivrent des **visas biométriques** aux ressortissants étrangers souhaitant voyager en France[5]. Ces documents correspondaient, depuis 2007, à des expérimentations dans certains pays. Depuis 2015, ils sont généralisés à l'ensemble des ressortissants des pays pour lesquels un visa est nécessaire pour entrer sur la zone Schengen.

---

[1] *Article 18 du décret n°2005-1726 du 30 décembre 2005 relatif aux passeports.*

[2] *Dotation forfaitaire des titres sécurisés créée par l'article 136 de la loi de finances pour 2009 et représentant un coût annuel de 18,28 millions d'euros pour l'État.*

[3] *Source : Agence nationale des titres sécurisés (ANTS).*

[4] Cf. *par exemple l'article R. 611-8 du code de l'entrée et du séjour des étrangers et du droit d'asile concernant le système VISABIO.*

[5] *Décret n° 2007-1560 du 2 novembre 2007 portant création d'un traitement automatisé.*

La prise des empreintes exige une **comparution personnelle** des demandeurs. Initialement, la biométrie a été expérimentée par des consulats délivrant un nombre relativement faible de visas. Puis, pour des pays plus importants où l'exigence de comparution personnelle engendrait une organisation différente de l'accueil des demandeurs, il a été fait appel à des **dispositifs d'externalisation** pour recevoir les demandeurs et prendre leurs empreintes.

Les empreintes digitales des dix doigts recueillies lors de la demande de visa sont conservées pendant cinq ans dans la base de données **VISABIO**. Cette dernière est reliée au système d'information sur les visas (VIS) qui comporte des données comparables mais recueillies par les autres États de l'Union européenne. Depuis début 2015, il est théoriquement possible, pour un demandeur dont les empreintes sont déjà enregistrées dans la base VIS[1], d'éviter une comparution personnelle lors d'une nouvelle demande de visa.

1 849 632 visas biométriques ont été délivrés par les autorités diplomatiques et consulaires en 2014 et la base VISABIO contient 9 millions de dossiers biométriques.

Le deuxième dispositif applicable aux ressortissants étrangers est le **système EURODAC**.

Il s'inscrit dans la logique du règlement européen *Dublin III*[2] fixant le principe selon lequel l'État membre responsable de l'examen d'une demande d'asile est le premier pays par lequel le demandeur a transité.

Les empreintes du ressortissant étranger concerné sont enregistrées dans la **base EURODAC.** Les États membres peuvent ensuite les comparer avec les autres données de ce fichier pour vérifier que l'étranger n'a pas formulé une **demande d'asile** dans un autre pays ou n'est pas **entré sur le territoire de l'Union de manière irrégulière**. Une procédure de transfert vers « *l'État responsable* » est engagée le cas échéant.

[1] *Enregistrement effectué par les services consulaires français, par d'autres pays européens ou par des prestataires de service.*

[2] *Règlement n° 604/2013 du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride.*

EURODAC distingue, concrètement, trois catégories d'étrangers :

	Catégorie 1	**Catégorie 2**	**Catégorie 3**
Étrangers concernés	Demandeurs d'asile	Étrangers interpellés lors du franchissement irrégulier d'une frontière extérieure de l'UE	Étrangers séjournant illégalement sur le territoire d'un État membre
Procédure suivie	Enregistrement et comparaison des empreintes digitales		Comparaison avec les données de la catégorie 1
Administration responsable	Préfectures	Direction centrale de la police aux frontières (DCPAF), uniquement à Roissy–Charles de Gaulle et Orly	Direction centrale de la police aux frontières (DCPAF) et préfectures
Durée de conservation des données	10 ans	18 mois	Pas de conservation

Source : commission des lois du Sénat à partir des éléments transmis par la Direction centrale de la police aux frontières (DCPAF)

En pratique, ces vérifications de la base EURODAC soulèvent des difficultés dans la mesure où :

- **certains États membres ne la renseignent pas systématiquement.** D'après la commission européenne, seuls 23 % des franchissements irréguliers d'une frontière extérieure de l'Union feraient l'objet d'un prélèvement d'empreintes digitales[1]. Cette négligence est due soit à un afflux exceptionnel d'entrées irrégulières, comme en Grèce en 2015, soit à la volonté de ne pas enregistrer une personne pour éviter ensuite qu'elle ne soit « *réadmise* » postérieurement dans le pays si elle est interpellée ou fait une demande d'asile dans un autre pays de l'Union européenne. Ce constat est toutefois à l'origine de nombreux efforts de l'Union européenne et de l'agence Frontex, pour parvenir à un enregistrement systématique des arrivées dans EURODAC ;

[1] *Communication COM (2015) 675 relative au rapport semestriel sur le fonctionnement de l'espace Schengen, 15 décembre 2015, p. 4 (https://ec.europa.eu/transparency/regdoc/rep/1/2015/FR/1-2015-675-FR-F1-1.PDF).*

- **le nombre de bornes EURODAC** – dispositif permettant le recueil des données et leur comparaison – **demeure limité** en raison de leur coût (30 000 euros par appareil). La Direction centrale de la police aux frontières (DCPAF) ne dispose par exemple que de quatorze machines de ce type sur l'ensemble du territoire. Elle envisage d'acquérir des capteurs biométriques plus légers et moins onéreux mais ayant des fonctionnalités moindres[1] ;

- **l'interface entre les bornes EURODAC et le fichier qui y est rattaché fonctionne mal** comme des sénateurs de la commission des lois ont pu le constater lors de leur déplacement en Grèce à l'hiver 2016[2].

Comparaison de données dans EURODAC

Source : commission européenne

Troisième outil à la disposition de l'administration, **l'application de gestion des dossiers des ressortissants étrangers en France (AGDREF 2)** permet l'instruction des demandes et la gestion des titres de séjour des ressortissants étrangers. Gérée par le ministère de l'intérieur, l'application conserve pendant cinq années les empreintes digitales des dix doigts :

- des demandeurs ou titulaires d'un titre de séjour ;

- des étrangers en situation irrégulière ou faisant l'objet d'une mesure d'éloignement[3].

[1] *Ces capteurs permettraient uniquement de consulter la base EURODAC pour les données de catégorie 3 (étrangers séjournant illégalement sur le territoire).*

[2] « L'Europe à l'épreuve de la crise des migrants : la mise en œuvre de la relocalisation des demandeurs d'asile et des hotspots », *rapport n° 422 (2015-2016) fait par François-Noël Buffet au nom de la commission des lois du Sénat, p. 23 (http://www.senat.fr/rap/r15-422/r15-4221.pdf).*

[3] *Article R. 611-2 du code de l'entrée et du séjour des étrangers et du droit d'asile.*

c) Des usages hybrides mêlant objectifs administratifs et judicaires

Cette distinction entre les objectifs administratifs et judiciaires de la biométrie a toutefois perdu en netteté avec le développement d'usages « *hybrides* ». Des techniques à visée d'abord administrative sont ainsi utilisées à des fins répressives et réciproquement.

Tel est le cas du fichier automatisé des empreintes digitales (**FAED**, finalité judiciaire) qui peut désormais être consulté pour identifier un étranger ne présentant pas ses documents de séjour ou ne communiquant pas les renseignements permettant l'exécution d'une mesure d'éloignement ou d'assignation à résidence (finalité administrative).

De manière comparable, le système **EURODAC** (finalité administrative) permet, depuis le règlement européen 603/2013 du 26 juin 2013, de comparer les données recueillies avec celles des autorités en charge de la répression des crimes (finalité judiciaire).

Ces croisements de fichiers biométriques demeurent toutefois très encadrés comme le prévoient :

- la jurisprudence du Conseil constitutionnel selon laquelle l'utilisation à des fins administratives de fichiers judiciaires ne doit pas, « *par son caractère excessif, porter atteinte aux droits ou aux intérêts légitimes des personnes concernées* »[1].

- le droit communautaire, comme le montre l'exemple du système EURODAC.

En effet, vu les possibilités ouvertes pour le traitement des données par les puissances de calculs disponibles et les capacités de stockage, ce type de traitement peut constituer de très lourds risques pour les libertés s'il n'est pas strictement encadré. Chaque autorisation d'utilisation d'un fichier doit s'accompagner de la mise en place de **garanties spécifiques pour les personnes.**

[1] *Conseil constitutionnel, décision n° 2003-467 DC du 13 mars 2003. En l'espèce, le fichier judiciaire automatisé des auteurs d'infractions sexuelles ou violentes (FIJAIS) peut être utilisé à des fins administratives pour vérifier le comportement des candidats à des emplois publics participant à la souveraineté de l'État.*

L'utilisation du système EURODAC à des fins répressives

Le **règlement européen 603/2013** précité encadre les conditions d'utilisation du système EURODAC à des fins répressives en définissant précisément les motifs de consultation et les autorités habilitées à cet effet.

La consultation à des fins répressives est uniquement envisageable pour « ***détecter ou prévenir*** » **des infractions terroristes**[1] **ou des** « ***infractions pénales graves*** »[2] (vols organisés ou avec arme, trafic de stupéfiants, *etc.*) passibles d'une peine de privation de liberté d'au moins trois ans.

En outre, **trois conditions cumulatives** doivent être remplies :

- **les bases de données nationales ont déjà été consultées** mais n'ont pas permis de déterminer l'identité de la personne recherchée ;

- une **affaire précise est concernée**, les « *comparaisons systématiques* » n'étant pas autorisées ;

- il existe des « ***motifs raisonnables de penser*** » **que la consultation contribuera** « ***de manière significative*** » **à la résolution d'une affaire criminelle**.

Pour obtenir les informations du système EURODAC, la police et la gendarmerie doivent s'adresser à un « ***service de vérification*** », seul compétent pour consulter le système à des fins répressives et ayant la responsabilité de vérifier que les trois conditions précitées sont respectées. Ce service correspond, en France, à la section centrale de coopération opérationnelle de police (SCCOPOL) de la direction centrale de la police judiciaire (DCPJ).

2. L'apport des techniques biométriques

L'apport des techniques biométriques est double : sécuriser l'identité des individus, d'une part, et rendre l'action administrative plus efficace, d'autre part.

a) Sécuriser l'identité des individus

Comme le rappelait notre ancien collègue Jean-René Lecerf, la biométrie présente, « *la particularité de permettre à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir* »[3].

Pour être exploitable par l'administration, une donnée biométrique doit toutefois répondre à quatre exigences : **l'universalité, l'unicité, la permanence et l'accessibilité.**

---

[1] *Telles que définies par les articles 1er à 4 de la décision-cadre 2002/475/JAI du Conseil du 13 juin 2002.*

[2] *Telles que définies à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil du 13 juin 2002.*

[3] « Identité intelligente et respect des libertés », *rapport d'information n° 439 (2004-2005) fait au nom de la mission d'information de la commission des lois du Sénat, p. 98 (https://www.senat.fr/rap/r04-439/r04-4391.pdf).*

Les quatre caractéristiques d'une donnée biométrique exploitable

Les données biométriques utilisées par l'administration pour sécuriser l'identité des personnes doivent être :

- **universelles** : ces données existent chez tous les êtres humains ;

- **uniques** : elles sont suffisamment discriminantes pour identifier une personne parmi des millions d'autres. À titre d'exemple, la probabilité de trouver deux empreintes digitales similaires est évaluée à 10^{-24} par l'Institut des systèmes intelligents et de la robotique[1] ;

- **permanentes** : les données restent globalement stables dans le temps et ne sont pas détériorées, par exemple par le vieillissement de la personne ;

- **accessibles** : elles peuvent être aisément prélevées sur le corps humain.

Source : « L'identité à l'ère du numérique », *Guillaume Desgens-Pasanau, Eric Freyssinet, août 2009, Éditions Presaje, p. 17.*

La sécurisation de l'identité et la lutte contre les fraudes à l'identité constituent un objectif de politique publique, ce qui explique l'utilisation croissante de la biométrie. Réprimées par le droit pénal[2], ces fraudes sont d'autant plus préoccupantes qu'elles peuvent servir de support à d'autres infractions comme l'usurpation d'identité, le crime organisé, l'escroquerie bancaire, *etc*.

La loi n° 2012-410 du 27 mars 2012[3] a prévu, dans cette logique, **la création d'une carte nationale d'identité biométrique** comportant les empreintes génétiques de son détenteur. À ce stade, ce dispositif n'a toutefois pas été mis en œuvre par le Gouvernement[4].

L'Observatoire national de la délinquance et des réponses pénales (ONDRP) distingue :

- les fraudes enregistrées par les services de police et les unités de gendarmerie : **5 910 faux documents d'identité saisis en 2014** ;

- les fraudes détectées par la direction générale de la police aux frontières (DCPAF) : **15 018 faux documents** interceptés cette même année. Dans la plupart des cas, ces documents sont contrefaits mais la DCPAF doit également faire face à des modifications indues de documents authentiques

[1] *Source : étude intitulée* « Reconnaissance automatique des empreintes digitales » *(p. 3) et disponible via le lien suivant :* http://www.isir.upmc.fr/UserFiles/File/LPrevost/Biometrie%20Empreintes.pdf.

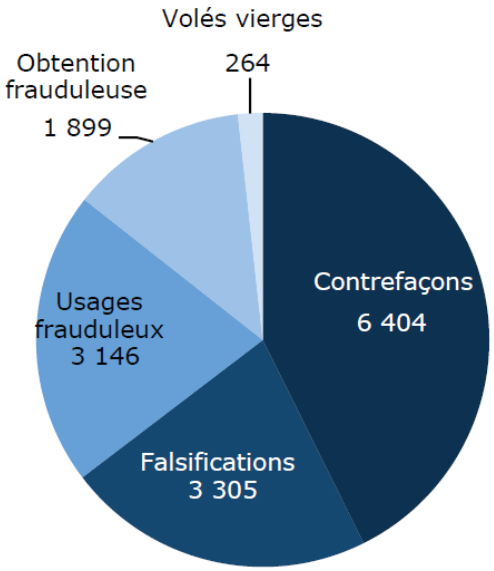
[2] *L'article 226-4-1 code pénal puni par exemple d'un an d'emprisonnement et de 15 000 € d'amende le fait d'usurper l'identité d'un tiers.*

[3] *Loi relative à la protection de l'identité.*

[4] Cf. *la seconde partie du présent rapport.*

(falsifications) ou à l'utilisation de documents d'identité par des tiers (usages frauduleux)[1].

Faux documents interceptés par la DCPAF en 2014



Source : Observatoire national de la délinquance et des réponses pénales

Dans le cas de la **frontière ferroviaire franco-britannique,** examiné par vos rapporteurs lors de leur déplacement à la gare du Nord le 24 mars 2016, **355 faux documents ont été détectés en 2015**, ce qui représente 0,004 % des 8,88 millions de passagers dénombrés[2]. **S'ils représentent un problème majeur, les cas de fraudes à l'identité ne doivent donc pas être surestimés.**

Hors Union européenne, des pays sont allés encore plus loin dans l'utilisation de la biométrie à des fins de sécurisation de l'identité des individus. De tels usages soulèveraient toutefois des difficultés en France au regard du droit au respect de la vie privée des citoyens.

[1] « Éléments de connaissance sur la fraude aux documents et à l'identité en 2014 », *Observatoire national de la délinquance et des réponses pénales, août 2015, p. 5-6* (*http://www.inhesj.fr/sites/default/files/files/ondrp_ra-2015/fraude_documents_cr.pdf*).

[2] *Source : Direction générale de la police aux frontières (DCPAF).*

Deux exemples internationaux : l'Inde et le Burkina Faso

Lancé en 2010, le **programme indien *Aadhaar*** vise à attribuer un numéro d'identification à chaque citoyen majeur. Dans une logique de sécurisation, ce numéro est relié aux données biométriques de la personne concernée (dix empreintes digitales et iris des yeux).

Le numéro Aadhaar est utilisé comme identifiant lors des relations administratives : il permet par exemple d'ouvrir une ligne téléphonique ou de recevoir des subventions. À ce stade, près d'un milliard d'Indiens se seraient vus affecter ce numéro.

Au **Burkina Faso**, la biométrie a été utilisée pour **fiabiliser les listes électorales** (*via* les empreintes digitales) et éviter toute « *double inscription* ». Opérationnel depuis les élections de décembre 2012, ce système a nécessité le déploiement de 3 500 stations d'inscription permettant d'enregistrer les données de 4,4 millions d'électeurs.

b) Rendre l'action administrative plus efficace

Les techniques biométriques s'inscrivent également dans la **« *transformation numérique* » des services publics,** appelée de ses vœux par la Cour des comptes dans une logique de simplification des relations entre les citoyens et l'administration[1].

La biométrie rend ainsi possible **l'automatisation des contrôles aux frontières et permet de concilier des vérifications approfondies, d'une part, et la forte croissance de la mobilité transfrontalière, d'autre part.**

Pour reprendre l'exemple de la Gare du Nord, 10 000 passagers partent chaque jour à destination du Royaume-Uni. Ce trafic a d'ailleurs vocation à s'accroître à moyen terme du fait de la mise en service de nouveaux trains permettant une hausse capacitaire de 20 %. Aux heures de pointe, 900 voyageurs devront ainsi être contrôlés en l'espace d'une demi-heure pour ne pas perturber le trafic[2].

La biométrie constitue donc, pour les gardes-frontières et les exploitants d'infrastructures de transport, une opportunité à saisir comme le démontre la mise en œuvre du **dispositif *« Passage automatisé rapide aux frontières extérieures »* (PARAFE).**

Prévu en 2007[3] et réellement opérationnel depuis novembre 2009, ce dispositif permet de réduire le temps d'attente à la frontière des Français et des citoyens de l'Union européenne munis d'un passeport biométrique. Il s'agit, pour les usagers, d'une procédure à la fois gratuite et facultative.

---

[1] « Relations aux usagers et modernisation de l'État : une généralisation des services publics numériques », *janvier 2016* (*https://www.ccomptes.fr/Publications/Publications/Relations-aux-usagers-et-modernisation-de-l-Etat*).

[2] *Source : société Eurostar.*

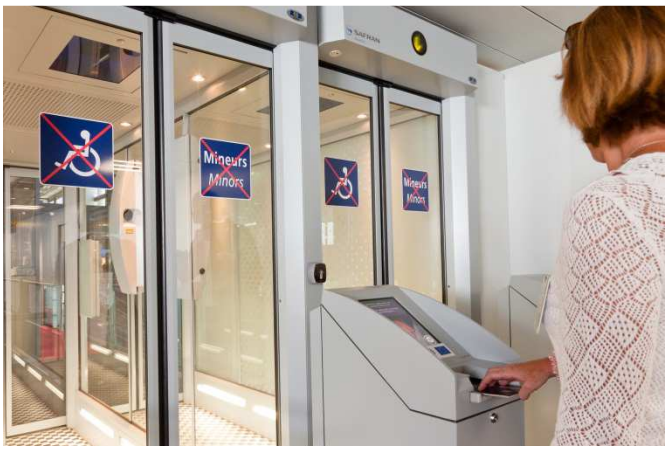
[3] *Décret n° 2007-1182 du 3 août 2007 portant création d'un traitement automatisé de données à caractère personnel relatives à des passagers des aéroports français franchissant les frontières extérieures des États parties à la convention signée à Schengen le 19 juin 1990.*

Concrètement, les voyageurs transitent par un **sas automatique** au lieu de passer devant un garde-frontière posté dans une aubette. Le **temps moyen de passage** dans un sas PARAFE est évalué à **20 secondes** et les données enregistrées (empreintes et photographies du passage dans le sas notamment) sont conservées pendant cinq ans[1].

Le garde-frontière remplit, pour sa part, une mission de supervision : surveillant plusieurs sas, il intervient si le passage est refusé par la machine ou en cas de doutes sur le comportement d'un usager.

Pour les personnes dont le passeport biométrique n'est pas un passeport français, une étape supplémentaire est nécessaire : en amont de cette procédure, la personne doit « *s'enregistrer* » dans une salle de l'aéroport ou de la gare prévue à cet effet. Cette différence s'explique par l'incapacité pour les sas français de « lire » l'ensemble des informations des passeports étrangers (*Cf.* infra).

Un sas PARAFE



Source : Safran identity and security

L'identité de l'usager est contrôlée en comparant les informations contenues dans son passeport biométrique et ses empreintes digitales.

[1] *Article R. 232-8 du code de la sécurité intérieure.*

Procédure PARAFE

Source : Direction centrale de la police aux frontières (DCPAF)

41 sas PARAFE sont aujourd'hui disponibles dans trois aéroports – Roissy-Charles de Gaulle (31 sas), Orly (6) et Marseille-Provence (4) – pour un coût unitaire estimé à 120 000 euros. Au 28 juin 2015, le système PARAFE avait déjà enregistré plus de 5,3 millions de passage.

B. UN NÉCESSAIRE ENCADREMENT JURIDIQUE

Si les techniques biométriques peuvent sécuriser l'identité des personnes et accroître l'efficacité de l'action administrative, leurs spécificités ainsi que des risques de fraudes et d'erreurs ont justifié l'émergence d'un cadre juridique spécifique.

1. Des données sensibles qui ne sont pas « des données à caractère personnel comme les autres »

Les données biométriques ne sont pas des *« données à caractère personnel comme les autres »* pour reprendre les mots de la Commission nationale de l'informatique et des libertés (CNIL).

En effet, *« à la différence d'une autre donnée d'identité (…),* ***la donnée biométrique n'est pas attribuée par un tiers ou choisie par la personne : elle est produite par le corps lui-même et le désigne ou le représente, lui et nul autre, de façon immuable.*** *Elle appartient donc à la personne qui l'a générée. (…) Confier ses données biométriques à un tiers, lui permettre de les enregistrer et de les*

conserver n'est donc jamais un acte anodin : cela doit répondre à une nécessité a priori *exceptionnelle, justifiée, et être entouré de garanties sérieuses* »[1]. Pour Antoinette Rouvroy, chercheure en philosophie du droit, la biométrie transforme **le corps en « *mot de passe* »** en partant du principe que « *le corps ne ment pas* »[2]. Le contrôleur européen des données considère, pour sa part, que « *la biométrie modifie définitivement la relation entre corps et identité* »[3].

a) Le cadre juridique européen et national

Le droit européen aborde les techniques biométriques en comparant leurs apports pour l'intérêt général, d'une part, et leurs effets sur la vie privée des personnes, d'autre part.

À titre d'exemple, la Cour européenne des droits de l'homme considère que **« *le fait que les profils ADN fournissent un moyen de découvrir les relations génétiques pouvant exister entre des individus suffit en soi pour conclure que leur conservation constitue une atteinte au droit à la vie privée de ces individus* »**. Cette atteinte doit ainsi être dûment justifiée par les autorités nationales. Tel n'est pas le cas du Royaume Uni lorsqu'il conserve des empreintes génétiques d'une personne acquittée par la justice : l'article 8 de la convention européenne des droits de l'homme (droit au respect de la vie privée et familiale) n'est pas respecté car cette mesure « *ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu* »[4].

Les données biométriques sont également encadrées par le droit communautaire car elles entrent dans le champ de **la directive 95/46/CE du 24 octobre 1995**[5] même si ce texte ne les mentionne pas explicitement. Le droit communautaire gagnera d'ailleurs en précision avec l'entrée en vigueur, à compter de 2018, de deux textes relatifs à la protection des données à caractère personnel.

---

[1] « Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données », *CNIL, décembre 2007, p. 3 (http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf).*

[2] *Citée dans* « Vie privée à horizon 2020 », *CNIL, 2012, p. 24 (https://www.cnil.fr/sites/default/files/typo/document/CNIL-CAHIERS_IPn1.pdf).*

[3] « Avis sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour », *Contrôleur européen des données, 23 mars 2005.*

[4] *Cour européenne des droits de l'homme, 4 décembre 2008,* S. et Marper c. Royaume-Uni *(n° 30562/04 et 30566/04).*

[5] *Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.*

Les techniques biométriques dans les textes communautaires applicables à compter de 2018

L'Union européenne a publié un paquet législatif visant à réformer la protection des données à caractère personnel et donc à remplacer la directive 95/46/CE précitée.

Publiée le 27 avril dernier, cette initiative législative comprend :

- **le règlement (UE) 2016/679** relatif à la protection des personnes physiques à l'égard du traitement **des données à caractère personnel** et à la libre circulation de ces données ;

- **la directive (UE) 2016/680** portant sur le traitement des données à caractère personnel à des fins de **prévention et de détection des infractions pénales.**

Ces deux textes qualifient les données biométriques de « ***catégories particulières de données à caractère personnel*** » et prévoient, dès lors, des garanties spécifiques.

Les traitements de données biométriques sont, par principe, interdits hors des usages de prévention et de détection des infractions pénales[1].

Des **exceptions sont toutefois prévues**, les traitements biométriques étant notamment permis lorsqu'ils sont *« nécessaires à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique »* ou justifiés par *« des motifs d'intérêt public important »*. Ces exceptions peuvent être interprétées strictement par les États membres et *« des conditions supplémentaires »*, y compris des limitations, sont possibles.

La logique est inverse concernant la prévention et la détection des infractions pénales[2]. Les traitements de données biométriques sont permis sous réserve :

- qu'ils soient autorisés par le droit de l'Union ou le droit d'un État membre ;

- et qu'ils permettent de protéger des intérêts vitaux ou portent sur des données manifestement rendues publiques par la personne concernée.

En dernier lieu, le règlement et la directive précités **encadrent les techniques biométriques « *comportementales* » ou de « *profilage* »**[3]. Hors la sphère pénale, la personne concernée *« a le droit de ne pas faire l'objet d'une décision fondée exclusivement »* sur ces techniques sauf si ces dernières sont prévues par le droit national ou de l'Union et si elles font l'objet *« de mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée »*[4].

À l'échelon national, les usages publics de la biométrie sont régis par **l'article 27 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.** Ils **sont autorisés par décret en Conseil d'État pris après avis motivé et publié de la CNIL.**

---

[1] *Article 9 du règlement (UE) 2016/679 précité.*

[2] *Article 10 de la directive (UE) 2016/680 précitée.*

[3] *Le* « profilage » *étant défini comme* « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données (…) pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne ».

[4] *Article 22 du règlement (UE) 2016/679 précité.*

Dans ses avis – qui demeurent consultatifs en l'espèce –, la **CNIL** considère que l'utilisation de la biométrie est légitime pour s'assurer de l'identité d'une personne.

Elle **met cependant en garde contre certaines difficultés soulevées par ce type de techniques**[1]. L'autorité administrative indépendante s'est, par exemple, montrée très réservée lors de la création d'un fichier central comportant les empreintes digitales des passeports biométriques, sans toutefois être suivie par le Gouvernement[2].

La CNIL procède également à des **vérifications *a posteriori*** des fichiers biométriques dans le cadre fixé par les articles 11 et 44 de la loi n° 78-17 précitée. Pour reprendre l'exemple des passeports, la CNIL a lancé un programme de vérification en 2012 pour s'assurer de l'enregistrement de seulement deux empreintes[3] dans la base des titres électroniques sécurisés (TES) et de l'effacement des empreintes « *surnuméraires* ».

b) Les garanties nécessaires : l'application des principes de finalité et de proportionnalité

Les traitements biométriques doivent **comporter des garanties permettant d'atteindre un équilibre entre leurs finalités** – que le pouvoir législatif ou réglementaire doit clairement expliciter –, **et le droit à la vie privée.**

Le Conseil constitutionnel synthétise cette « ***grille d'analyse*** » par un considérant de principe selon lequel « *la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée ; (…) par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être* ***justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif*** ».

À l'occasion d'une question prioritaire de constitutionnalité[4], le Conseil a ainsi considéré que **le fichier national automatisé des empreintes génétiques (FNAEG) respecte cet équilibre** dans la mesure où :

- sa finalité est suffisamment précise et répond à un motif d'intérêt général : faciliter la recherche des auteurs de certaines infractions ;

- des garanties sont prévues pour encadrer l'utilisation de ce fichier et s'assurer, ainsi, du respect du principe de proportionnalité : le contrôle du FNAEG relève de la CNIL et d'un magistrat de l'ordre judiciaire, le fichier s'inscrit dans le cadre de procédures judiciaires, les personnes concernées

[1] *Cf. infra et notamment les développements sur les risques d'erreurs et de fraudes.*
[2] *Délibération n° 2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.*
[3] *Conformément à l'arrêt du 26 octobre 2011 dans lequel le Conseil d'État a annulé une disposition du décret du 30 décembre 2005 précité et prévoyant l'enregistrement de huit empreintes digitales.*
[4] *Conseil constitutionnel, décision n° 2010-25 QPC du 16 septembre 2010.*

ont un droit d'accès et peuvent demander la rectification d'informations erronées, *etc.*

À l'inverse, un tel équilibre n'a été que partiellement atteint par la loi n° 2012-410 du 27 mars 2012[1]**.**

Telle qu'adoptée par le Parlement, cette loi prévoyait principalement :

- la **création d'une carte d'identité** dotée d'une puce électronique contenant plusieurs données à caractère personnel dont **deux empreintes digitales**. Cette carte aurait pu être utilisée à des fins commerciales (régler des transactions, notamment dans le cadre d'une prestation de commerce en ligne) et administratives (développer l'administration électronique) ;

- la constitution d'un « ***fichier central commun*** » intégrant les données des cartes d'identité et des passeports biométriques.

Dans sa décision n° 2012-652 DC du 22 mars 2012, **le Conseil constitutionnel n'a pas contesté la possibilité de créer une carte d'identité biométrique**. Il a toutefois **censuré** deux éléments de la loi n° 2012-410 précitée : **son utilisation à des fins commerciales** (pour un motif procédural d'incompétence négative)[2] **et la constitution du « *fichier central commun* »** (pour un motif de fond, le non-respect du principe de proportionnalité).

Le Conseil a considéré que cette base de données porterait au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée eu égard à *« l'ampleur de ce fichier, à ses caractéristiques techniques et aux conditions de sa consultation »*.

Le commentaire de la décision indique, plus précisément, que le Conseil constitutionnel s'est appuyé sur **quatre arguments** pour constater l'insuffisance des garanties prévues :

- la taille très importante de ce traitement de données qui aurait compris les données de la quasi-totalité de la population française ;

- la pluralité de ses finalités (identification administrative, besoins de la prévention et de la répression des atteintes à l'indépendance de la Nation, *etc.*) ;

- le caractère particulièrement sensible des données biométriques ;

---

[1] *Loi relative à la protection de l'identité.*

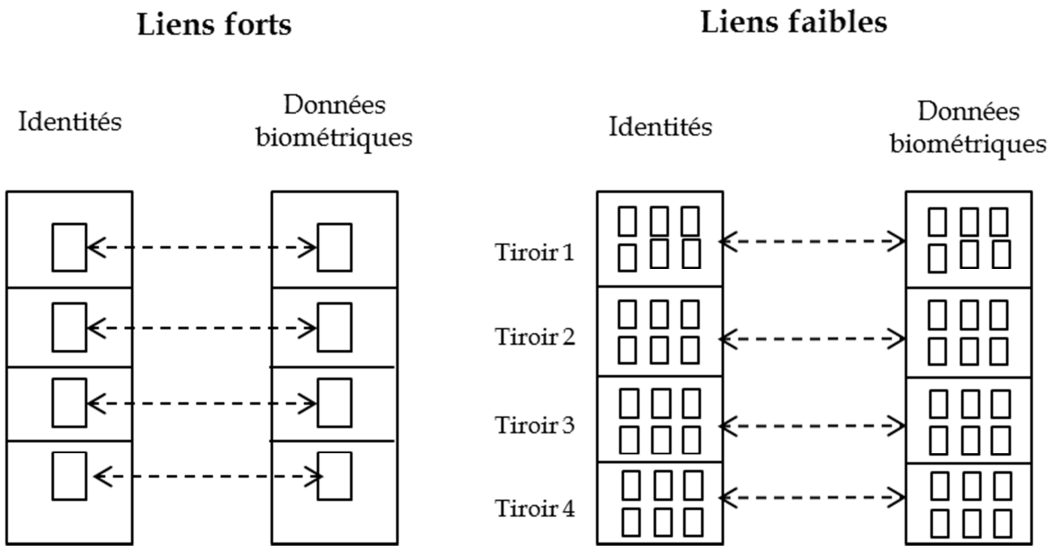
[2] *Le Conseil estime en effet que le législateur a* « méconnu l'étendue » *de la compétence que lui confère l'article 34 de la Constitution dans la mesure où il n'a pas défini la nature des données permettant cette identification électronique, les garanties mises en œuvre pour assurer leur intégrité et leur confidentialité ainsi que les conditions d'authentification des personnes.*

- la possibilité d'identifier une personne par une technique de « ***liens forts*** », disposition de la loi adoptée contre la position du Sénat qui privilégiait des « *liens faibles* »[1].

La distinction entre les fichiers à « *liens forts* » et ceux à « *liens faibles* »

Dans un traitement biométrique à « ***liens forts*** », **une donnée est reliée à une identité**, ce qui permet d'établir très rapidement une correspondance entre ces deux informations. Bien que certains traitements soient « *unidirectionnels* » (retrouver une empreinte à partir d'une identité mais non l'inverse par exemple), il est toujours possible de procéder à des recoupements et ainsi d'interroger la base dans les deux sens.

Dans un système à « ***liens faibles*** », **un nombre très élevé d'identités est relié aux données biométriques correspondantes**, sans qu'aucun lien univoque ne soit établi entre l'une de ces identités et l'une de ces données biométriques. Les biométries correspondent, par exemple, à 100 000 identités rangées dans un « *tiroir* » unique et il est techniquement très difficile de retrouver une identité à partir d'une simple information biométrique. La technique des « *liens faibles* » représente donc une **garantie supplémentaire** pour les personnes inscrites dans le fichier concerné.



Source : commission des lois du Sénat

2. Des risques d'erreurs et de fraudes

Même si elles sont propres à chaque individu, les données biométriques ne sont pas infaillibles : des risques d'erreurs et de fraudes

[1] *Rapport n° 432 (2010-2011) de M. François Pillet relatif à la proposition de loi* « protection de l'identité » *fait au nom de la commission des lois du Sénat, p. 38* (*https://www.senat.fr/rap/l10-432/l10-4321.pdf*).

persistent. Notre ancien collègue Jean-René Lecerf invitait ainsi à « ***ne pas surestimer la fiabilité de la biométrie*** »[1].

a) Des risques d'erreurs

S'agissant tout d'abord des risques d'erreurs des techniques biométriques, deux variables doivent être prises en compte :

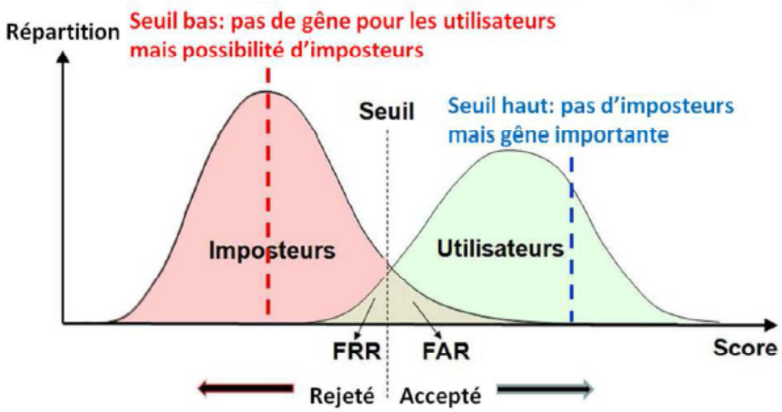
- **le taux de fausses acceptations (FAR)** : le système n'arrive pas à reconnaître un imposteur et à le rejeter ;

- **le taux de faux rejets (FRR)** : le système ne parvient pas à identifier une personne éligible et la rejette à tort.

À titre d'exemple, les **dispositifs de reconnaissance digitale** de la Direction générale de la police aux frontières (**DCPAF**) présentent **un FAR de 0,1 % et un FRR de 3 %.**

Ces **deux taux** sont **interdépendants** et diffèrent d'un dispositif biométrique à l'autre : réduire le taux de fausses acceptations pour diminuer les risques « *d'impostures* » conduit mécaniquement à accroître le taux de faux rejet. Cet arbitrage est réalisé à l'occasion de la configuration des algorithmes de vérification des dispositifs biométriques.

Le réglage des dispositifs biométriques : l'arbitrage entre FAR et FRR



Source : « Évaluation de systèmes biométriques », *Mohamad El Abed, thèse soutenue à l'université Caen Basse-Normandie le 9 décembre 2011, p. 28.*

Baisser le seuil de sécurité revient, comme le montre ce schéma, à réduire le nombre de faux rejet (et donc la gêne occasionnée pour les usagers) mais à accroître les fausses acceptations (et donc le risque d'impostures).

[1] « Identité intelligente et respect des libertés », *rapport d'information n° 439 (2004-2005) fait au nom de la mission d'information de la commission des lois du Sénat, p. 69 (https://www.senat.fr/rap/r04-439/r04-4391.pdf).*

La fiabilité des techniques biométriques dépend, en outre, du **rythme de transformation du corps humain**. Comme le soulignent MM. Guillaume Desgens-Pasanau et Eric Freyssinet, la biométrie présente *« un inconvénient majeur : aucune mesure d'une donnée biométrique par un système informatique ne se révèle être totalement exacte car le corps vieillit et il subit au fil du temps un certain nombre d'altérations voire de traumatismes »*[1].

La biométrie s'avère, enfin, **inopérante lorsqu'il est techniquement impossible de prélever une donnée** sur un corps humain. À titre d'exemple, 3 % de la population ne pourraient se voir prélever leurs empreintes digitales[2] du fait, par exemple, de l'usage répété de produits corrosifs.

b) Des risques de fraudes

Les tentatives de fraudes ne sont pas à exclure lors de l'utilisation de dispositifs biométriques.

Il existe, tout d'abord, un **risque lors de la captation des données** (phase *« d'enrôlement »*). En effet, si une identité erronée est rattachée à une donnée biométrique, cette erreur ne pourra être détectée lors de vérifications ultérieures.

Diverses techniques sont également possibles pour *« tromper »* les dispositifs biométriques dont le ***« morphing »*** (conception d'un visage de synthèse pour abuser les outils de reconnaissance faciale) ou les ***« faux doigts »*** (fabrication d'un doigt artificiel imitant l'empreinte digitale d'un tiers).

Ainsi, l'empreinte digitale de Mme Ursula von der Leyen, ministre de la défense allemande, a pu être imitée par un informaticien en décembre 2014 et des journalistes ont trompé les sas PARAFE dans le cadre d'un reportage diffusé en septembre 2015 sur une chaîne du service public[3].

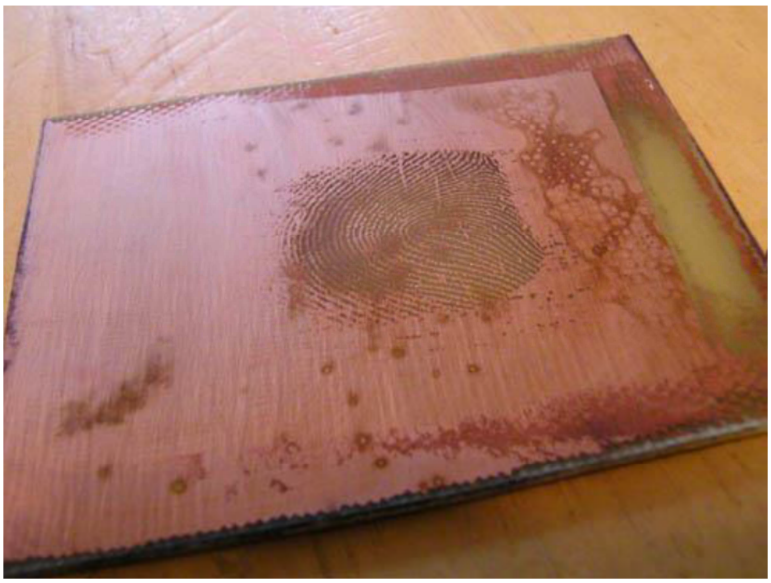
---

[1] « L'identité à l'ère du numérique », *Guillaume Desgens-Pasanau, Eric Freyssinet, août 2009, Éditions Presaje, p. 43.*

[2] *Source :* « L'identification biométrique : champs, acteurs, enjeux et controverses », *Ayse Ceyhan et ali., juin 2011, Éditions Broché, p. 249.*

[3] « Le business de la peur », *reportage de Jean-Pierre Canet diffusé dans l'émission « Cash investigation » (France Télévisions) le 21 septembre 2015.*

Un « *faux doigt* »



Source : « Hacking biométrie :
tromper un scanner d'empreintes digitales »,
Centre national de recherche scientifique (CNRS), mars 2013.

La CNIL rappelle, enfin, qu'un traitement centralisé de données biométriques peut présenter des **risques en termes de sécurité informatique**, étant *« d'autant plus vulnérable et susceptible d'utilisations multiples qu'il est de grande dimension, qu'il est relié à des milliers de points d'accès et de consultation, et qu'il contient des informations très sensibles »*[1].

L'ensemble de ces risques nécessite donc la mise en œuvre de sécurités particulières et des avancées technologiques sont encore possibles pour réduire le risque de fraude.

II. LES POTENTIALITÉS DES DISPOSITIFS BIOMÉTRIQUES POURRAIENT ÊTRE DAVANTAGE EXPLOITÉES SOUS RÉSERVE DE LA NÉCESSAIRE PROTECTION DE LA VIE PRIVÉE

Les autorités publiques recourent de manière croissante aux techniques biométriques pour s'assurer de l'identité des personnes et accroître l'efficacité de l'action administrative.

Les **avancées techniques constatées** par vos rapporteurs **conduisent** toutefois à **envisager le développement de nouveaux usages de la biométrie** pour simplifier les relations administratives et mieux gérer les frontières extérieures de l'espace Schengen. La connexion entre des dispositifs de

[1] « Note d'observations concernant la proposition de loi relative à la protection de l'identité », *CNIL, 25 octobre 2011, p. 4* (*https://www.cnil.fr/sites/default/files/typo/document/CNIL-PPLidentite-Noteobservations-25-10-2011.pdf*).

vidéoprotection et certaines bases de données pourrait également être expérimentée afin de vérifier en phase opérationnelle les nouvelles possibilités offertes par les technologies de reconnaissance faciale. Ceci pourrait ainsi permettre **une surveillance de l'accès à des zones sensibles (aéroports, grands rassemblements, *etc.*) sans imposer de manière systématique le passage sous des portiques de sécurité**. Les files d'attente en amont des portiques – très difficiles à sécuriser par nature – seraient dès lors réduites.

A. SIMPLIFIER LES RELATIONS ADMINISTRATIVES

Exploiter davantage les potentialités des techniques biométriques pourrait participer à la fluidification des relations entre les citoyens et leur administration.

Il s'agit, plus précisément, de faciliter et de sécuriser l'identité numérique mais aussi de poursuivre la modernisation des procédures de délivrance de visas et de passeports biométriques.

1. Faciliter et sécuriser l'identité numérique

À ce jour, les Français ne disposent pas d'une identité numérique fiable et utilisable dans leurs relations avec l'administration, le Gouvernement n'ayant pas souhaité développer la carte nationale d'identité biométrique prévue par la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité et dont la création a été validée par le Conseil constitutionnel[1].

a) Les mesures alternatives mises en œuvre par le Gouvernement

Mettant en exergue le coût que représenterait l'émission de cartes d'identité biométriques (environ 85 millions d'euros), **l'exécutif** considère qu'il ne « *s'agit plus (…) d'un chantier prioritaire* »[2] et **privilégie des mesures alternatives**.

La première mesure consiste à lutter contre la fraude en **sécurisant les procédures de détermination de l'identité d'une personne et en détectant plus rapidement les faux documents**.

Trois programmes répondant à cette logique sont en cours de déploiement : **Communication électronique des données publiques (COMEDEC), 2D-DOC et CHECKDOC.**

---

[1] Cf. *la première partie du présent rapport, le Conseil n'ayant censuré que le* « fichier central commun » *et l'utilisation de cette carte d'identité à titre commercial.*

[2] *Questions n° 4746 du 18 novembre 2012 de M. Philippe Meunier (réponse publiée le 1er janvier 2013) et n° 47385 du 7 janvier 2014 de Mme Valérie Boyer (réponse publiée le 25 novembre 2014).*

Les programmes de sécurisation de l'identité

	COMEDEC	2D-DOC	CHECKDOC
Finalités	Assurer l'authenticité des actes d'état civil	S'assurer que des faux documents ne sont pas utilisés, notamment pour les relations commerciales	Mieux détecter les faux documents lors des contrôles des forces de l'ordre
Principe de fonctionnement	Échange dématérialisé de données d'état civil entre une administration ou un notaire demandeurs et le service conservant ces données, l'administré n'intervenant pas durant cet échange	Apposition par l'émetteur du document d'un code à barres sécurisé contenant les données protégées (nom du récepteur du document, adresse, *etc*.)	Dispositif mobile permettant de vérifier que le document n'a pas été volé ou perdu et qu'il n'est pas périmé
Documents concernés	Actes de naissance	Documents pouvant servir de justificatifs de domicile (soit 15 millions de documents potentiels)[1]	Documents d'identité
Entités et personnes concernées	- Demandeurs : administrations et notaires - Dépositaires des données : service de l'état civil de la commune de naissance	- Émetteurs : les entreprises ou administrations volontaires - Récepteurs : les administrations ou entreprises souhaitant s'assurer de l'authenticité du document	- Utilisateurs : forces de police et de gendarmerie ; - Personnes contrôlées : les citoyens
Base juridique	- Décret n° 2011-167 du 10 février 2011[2]; - Arrêté technique du 23 décembre 2011	- Arrêté du 27 septembre 2013[3]	Cadre juridique général des contrôles d'identité
Administrations en charge du programme	Ministère de la justice et ANTS	Ministère de l'intérieur et ANTS	
Périmètre	Dispositif facultatif pour les communes (environ 250 municipalités équipées)	Dispositif facultatif pour les entreprises et administrations	En cours de déploiement dans les services des forces de l'ordre

Source : commission des lois du Sénat

Parallèlement, **l'Agence nationale des titres sécurisés (ANTS) développe le projet ALICEM**, prototype qui devrait être opérationnel à compter de l'été 2017.

Il s'agirait, pour les citoyens, de certifier leur identité à partir de leurs données biométriques et d'accéder, ainsi, à des services administratifs ou commerciaux en ligne.

---

[1] *Estimation de la direction de la modernisation et de l'action territoriale du ministère de l'intérieur.*

[2] *Décret instituant une procédure de vérification sécurisée des données à caractère personnel contenues dans les actes de l'état civil.*

[3] *Arrêté relatif à la sécurisation des pièces justificatives de domicile requises pour la délivrance d'un titre d'identité au moyen d'un dispositif électronique propre à garantir l'authenticité.*

Fonctionnement du prototype ALICEM

Pour utiliser ce dispositif, le citoyen devrait avoir en sa possession : **un téléphone portable type « *smartphone* » et un passeport biométrique**. Il devrait également télécharger **l'application ALICEM**, mise gratuitement à disposition par l'ANTS.

Le citoyen créerait ensuite son « ***identité ALICEM*** » en respectant la procédure suivante :

a) ouvrir l'application, entrer un mot de passe choisi librement, un numéro de téléphone portable et une adresse électronique ;

b) entrer le code envoyé automatiquement par l'application au numéro de téléphone indiqué par l'usager ;

c) renseigner les informations relatives à son passeport (numéro et date d'expiration du document, date de naissance) ;

d) **prise d'une photographie à partir du téléphone pour que l'application contrôle que la personne demandeuse est bien le détenteur du passeport (reconnaissance faciale).**

Une fois cette identité créée, le citoyen pourrait facilement accéder à l'application à partir de son mot de passe et d'une nouvelle reconnaissance faciale. Son identité étant vérifiée, il pourrait procéder à **diverses procédures administratives et commerciales en ligne** (payer ses impôts, signer un contrat, *etc.*). Un contact avec le passeport serait nécessaire pour toute transaction dans une logique de sécurisation. L'application vérifierait également que le portable et le passeport n'ont fait l'objet d'aucune déclaration de vol.

L'application ALICEM ne génèrerait **aucune base de données**. À terme, ALICEM pourrait également fonctionner à partir des titres de séjour ou d'une carte d'identité électronique.

Vos rapporteurs soutiennent l'ensemble de ces initiatives en cours de déploiement dans la mesure où elles permettent de sécuriser l'identité des citoyens et qu'il est confirmé qu'elles constituent une première étape vers une identité numérique fiable. Ils espèrent qu'elles seront rapidement généralisées afin que les Français puissent se les approprier dans leur vie quotidienne.

Proposition n° 1 : Poursuivre le développement de l'identité numérique utilisant des données biométriques (ALICEM), comme envisagé par l'ANTS, en valider la fiabilité et travailler à son indispensable encadrement juridique.

Coordonner cette démarche avec les autres initiatives européennes.

b) La création d'une carte d'identité biométrique

Si elles apparaissent positives, **les initiatives du Gouvernement ne se substituent pas à la création d'une carte d'identité biométrique, que vos rapporteurs appellent de leurs vœux.** Ils rejoignent en cela une préconisation de la Cour des comptes qui a proposé de « *réétudier l'opportunité de développer une carte nationale d'identité électronique* »[1].

En effet, **la position prise par le législateur lors de la loi n° 2012-410 du 27 mars 2012 n'a pas perdu en acuité** : la biométrie représente un moyen fiable pour sécuriser les documents d'identité et lutter contre les fraudes.

En outre, quatre ans après l'adoption de cette loi, de nouveaux arguments plaident en faveur de la création d'une telle carte d'identité biométrique reliée à un fichier à « *liens faibles* ».

Vos rapporteurs observent, tout d'abord, que **le passeport biométrique a été généralisé sans que cela ne soulève de difficulté en termes d'acceptation sociale**.

Ils rappellent également que **la procédure de délivrance de la carte d'identité fait déjà l'objet d'un relevé d'empreintes digitales** et que ces dernières peuvent être utilisées « *en vue de la détection des tentatives d'obtention ou d'utilisation frauduleuse d'un titre d'identité (et) de l'identification certaine d'une personne dans le cadre d'une procédure judiciaire* »[2].

Ce **recueil papier** – et donc « *artisanal* » – des empreintes représente une **charge de travail non négligeable pour les services municipaux et préfectoraux** qui ont édité environ 4,5 millions de cartes d'identité en 2014[3]. Or, en l'état des pratiques, les résultats de ce travail **ne sont pas exploités,** les empreintes n'étant pas enregistrées dans un traitement informatique permettant l'identification des personnes.

En outre, **la base de données relative aux cartes nationales d'identité est aujourd'hui obsolète et peu fonctionnelle** comme l'ont montré les auditions de vos rapporteurs.

Sa modernisation pourrait donc représenter l'occasion de mieux traiter les empreintes digitales recueillies pour la délivrance de la carte d'identité tout en respectant la jurisprudence du Conseil constitutionnel. Il s'agirait, en particulier, **de prévoir un fichier à « *liens faibles* »** – et non à liens forts – comme le préconisait notre collègue François Pillet en 2012.

---

[1] « Relations aux usagers et modernisation de l'État. Vers une généralisation des services publics numériques », *Cour des comptes, Janvier 2016, p. 88-89* (*https://www.ccomptes.fr/Publications/Publications/Relations-aux-usagers-et-modernisation-de-l-Etat*).

[2] *Article 5 du décret n°55-1397 du 22 octobre 1955 instituant la carte nationale d'identité.*

[3] « Administration générale et territoriale de l'État », *annexe 3 au rapport n° 3110 sur le projet de loi pour 2016 fait par M. Romain Colas, p. 26* (*http://www.assemblee-nationale.fr/14/budget/plf2016/b3110-tIII-a3.asp#P623_59421*).

D'après plusieurs personnes entendues en audition, **le Gouvernement étudierait une mesure alternative dans le cadre du plan « *préfectures nouvelle génération* »** annoncé par le ministre de l'intérieur le 9 juin 2015. Il s'agirait de **fusionner le fichier « *TES* »** – recueillant les informations relatives aux passeports – **et le fichier des cartes nationales d'identité.** La **faisabilité** de ce projet semble toutefois très **incertaine** sur un plan tant technique (comment mêler ces deux fichiers dont les finalités et le contenu diffèrent ?) et juridique (cette fusion ne reviendrait-elle pas à contourner la décision n° 2012-652 DC précitée et censurant le « *fichier central commun* » ?).

Vos rapporteurs constatent, enfin, que **de nombreux États délivrent déjà des cartes d'identité biométrique** et que ces dernières sont parfois reliées à une base de données (Espagne, Pays-Bas et Lituanie).

Exemple d'États ayant recours à des cartes d'identité biométrique

	Collecte d'empreinte	Base de données	Date de lancement
Allemagne	Facultative	Non	2010
Espagne	Obligatoire	Oui	2006
Italie	Obligatoire	Non	-
Royaume Uni	Non	Non	-
Belgique	Non	Non	2005
Pays-Bas	Obligatoire	Oui	2014
Portugal	Obligatoire	Non	2007
Suède	Non	Non	-
Finlande	Non	Non	-
Lituanie	Oui	Oui	2009

Source : commission des lois du Sénat et CNIL

Pour relancer la carte nationale d'identité biométrique, il conviendrait de **s'inspirer des caractéristiques du passeport**. Les **usages commerciaux seraient** ainsi **exclus** du dispositif et seraient gérés par le programme ALICEM ; les données biométriques conservées se limiteraient à deux empreintes digitales.

La détention de cette carte resterait facultative dans la logique du droit en vigueur, l'identité d'une personne pouvant être prouvée « *par tout moyen* »[1].

[1] *Article 1er de loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité.*

Proposition n° 2 : Pour permettre à l'État de garder l'initiative en matière d'identification et lutter contre les usurpations d'identité, créer une carte nationale d'identité biométrique, conformément à la logique de la loi n° 2012-410 du 27 mars 2012, et présentant les caractéristiques suivantes :

- conservation de deux empreintes digitales ;

- lien avec un fichier comprenant des « liens faibles » ;

- exclusion des usages commerciaux et notamment des possibilités d'achats en ligne.

Dans la même logique, il semble nécessaire de **recueillir les données biométriques des nouveaux titulaires du certificat de nationalité française (CNF)**.

Pour mémoire, ce document est délivré par le greffier en chef du tribunal d'instance et sert à démontrer que la personne possède la nationalité française. Sa délivrance suppose la production d'un acte de naissance souvent rédigé par les services civils d'un État étranger.

Insérer un élément biométrique dans le certificat de nationalité française permettrait **de renforcer la fiabilité de la « *chaîne de l'identité* »**, notamment en comparant les biométries des CNF avec celles des passeports.

Proposition n° 3 : Recueillir les données biométriques des nouveaux titulaires de certificat de nationalité française, lors de la remise de leur CNF, et les introduire dans le fichier des passeports pour lutter contre la fraude documentaire.

2. Poursuivre la modernisation des procédures de délivrance des passeports et des visas biométriques

Si la biométrie peut simplifier les relations entre les citoyens et l'administration, elle soulève une difficulté majeure : **l'exigence d'une « *double comparution* »**.

La délivrance d'un titre d'identité biométrique nécessite, en effet, que la personne concernée se présente physiquement en vue du recueil de ses empreintes digitales puis pour le retrait du document quelques jours ou quelques semaines plus tard. Vos rapporteurs ont clairement constaté cette difficulté concernant la délivrance des passeports et des visas.

a) La délivrance des passeports biométriques

Pour les passeports, la double comparution – au moment de la demande, pour la prise des empreintes biométriques, puis à la remise du document pour vérifier l'adéquation entre la personne et les données

biométriques recueillies – représente une **difficulté parfois très coûteuse pour les Français établis hors de France et dont la résidence est géographiquement éloignée de leur ambassade et de leur consulat**[1].

C'est pourquoi, s'appuyant sur la pratique des autres pays européens, il a été accepté que le passeport d'un Français de l'étranger puisse non seulement être remis après une seconde comparution, mais aussi par un consul honoraire ou à l'occasion d'une tournée consulaire.

Le **décret n° 2015-701 du 19 juin 2015**[2] a prévu une facilité complémentaire : les Français de l'étranger pourront désormais obtenir à leurs propres frais[3] **l'envoi sécurisé** du passeport à leur domicile et éviter ainsi toute double comparution.

Ce dispositif n'est toutefois pas encore opérationnel : l'ANTS doit procéder à certains ajustements techniques alors que les ministères de l'intérieur et des affaires étrangères doivent publier[4] un arrêté conjoint d'application. **Vos rapporteurs souhaitent vivement que cette simplification devienne effective dès l'automne 2016, et ce dans un grand nombre de pays comme l'a annoncé le Gouvernement.**

À moyen terme, ces avancées pourraient intéresser l'ensemble des citoyens français, y compris ceux résidant sur le territoire national. Vos rapporteurs considèrent ainsi qu'il est **possible de réduire les déplacements nécessaires** aux citoyens **lors du renouvellement des passeports**, procédure pour laquelle un nouveau recueil d'empreintes est demandé en l'état du droit, alors que rien ne le justifie sur le plan technique.

b) La délivrance des visas biométriques

Depuis 2015, l'ensemble des ressortissants des pays étrangers dont le séjour est soumis à un visa doivent disposer de visas biométriques, les derniers pays à avoir « *basculé* » vers ce type de documents étant la Russie, la Chine, l'Inde (qui représentent à eux trois un tiers des demandes totales de visas), le Royaume Uni et l'Irlande.

Votre co-rapporteur, M. Jean-Yves Leconte, a fait part de ses inquiétudes au Gouvernement dès août 2014[5], **l'attractivité du territoire national** pouvant être réduite par le recueil de données biométriques et **ses implications en termes de comparution physique auprès d'un poste consulaire ou d'un prestataire de services « visa », parfois éloigné du lieu de résidence du voyageur potentiel**. En effet, « *l'obligation de faire enregistrer*

---

[1] *Les citoyens français établis sur le territoire national pouvant facilement s'adresser à une commune située à proximité de leur lieu de résidence* (Cf. *la première partie du présent rapport).*

[2] *Décret simplifiant la délivrance des passeports.*

[3] *Selon les informations recueillies par vos rapporteurs, le coût de cet envoi sécurisé pour les Français de l'étranger volontaires pourrait s'élever à 15 euros.*

[4] *Après avis de la Commission nationale de l'informatique et des libertés (CNIL).*

[5] Question orale n° 835, 22 juillet 2014 (réponse de M. André Vallini, secrétaire d'État chargé de la réforme territoriale).

ses empreintes entraîne de lourdes difficultés pour les candidats au voyage vers la France, obligés de se déplacer jusqu'à un consulat (…), parfois à des milliers de kilomètres de leur lieu de résidence. Ainsi, par exemple, après la mise en place de la biométrie en Indonésie, un archipel de 13 000 îles avec plus de 4 000 kilomètres de distance interne, l'obligation de passer par Djakarta a fait baisser les demandes de visas de plus de 35 % ». Cette situation s'est ensuite progressivement et partiellement redressée, mais n'aide pas à nos échanges. Concernant les visas de courts séjour, la possibilité, depuis début 2015, de réutiliser des empreintes déjà incluses dans la base VIS peut éviter une nouvelle comparution. **Les difficultés demeurent toutefois pour les titres de long séjour** dans les pays où les déplacements sont longs (Brésil) ou chers (Japon) ou dans ceux qui ne disposent pas d'un poste consulaire (Nicaragua).

Conscient de ce défi**, le Gouvernement s'est attaché à prévoir un maillage cohérent et efficace des centres de recueil de données biométriques**. La France compte ainsi 14 centres de ce type en Inde et 15 en Chine.

Conformément à l'article 43 du code communautaire Schengen, la France a pu externaliser certains de ses centres de collecte en faisant appel à des sociétés privées (VFS Global, TLS Services et Capago) dans les pays de taille importante et où le réseau consulaire n'a pas paru suffisant pour répondre de manière rationnelle à l'ensemble des demandes.

Certains d'entre eux sont **mutualisés** avec d'autres pays, ce qui accroît leur efficacité. Le centre de collecte ouvert en Algérie est par exemple utilisé par la France mais également par l'Italie.

Vos rapporteurs expriment des réserves sur certains aspects de l'externalisation en matière de sécurisation des données et rappellent les inquiétudes, pour certains demandeurs, de devoir passer par une société privée pour faire une demande de visa en France.

Ils saluent toutefois l'apport de cette politique à la qualité de l'accueil des demandeurs et au temps de traitement des demandes de visa et appellent à sa poursuite. Ils rejoignent ainsi la commission des finances de notre Haute assemblée dans son souhait de « *privilégier le choix de centres externalisateurs communs à d'autres pays de l'espace Schengen* » pour « *renforcer la coopération consulaire* »[1]. **Ils souhaitent aussi qu'une politique comparable soit développée pour les passeports biométriques** dont la délivrance est sollicitée par les Français de l'étranger afin que les demandes de passeport puissent se faire au plus près de leur lieu de vie.

La politique de délivrance des visas pourrait également évoluer de manière positive en **menant à leur terme les expérimentations de recueil mobile d'empreintes digitales**. Dans un tel schéma, les entreprises gérant les

[1] « Faire de la délivrance des visas un outil d'attractivité de la France », *rapport d'information n° 127 (2015-2016) de MM. Éric Doligé et Richard Yung, fait au nom de la commission des finances du Sénat, p. 40(https://www.senat.fr/rap/r15-127/r15-127.html).*

centres externalisés (VFS Global, TLS Services et Capago) se déplacent pour répondre à une demande de visas localisée (entreprises de grande taille, événement dans une ville donnée, *etc.*) et se rendent ainsi au plus près des personnes souhaitant voyager en France.

Proposition n° 4 : Poursuivre la modernisation des procédures de délivrance des passeports et des visas biométriques :

- mettre en œuvre l'envoi sécurisé des passeports des Français de l'étranger prévu par le décret n° 2015-701 du 19 juin 2015 ;

- éviter un nouveau recueil d'empreintes lors d'un renouvellement de passeport biométrique ;

- approfondir la politique de mutualisation de la collecte des données biométriques des visas et l'étendant aux passeports ;

- harmoniser au niveau européen les collectes de données biométriques incluses dans les passeports européens et pour les visas ;

- mener à son terme l'expérimentation de recueil mobile de ces données.

B. DÉVELOPPER L'USAGE DE LA BIOMÉTRIE AUX FRONTIÈRES

La gestion des frontières constitue la sphère administrative dans laquelle les techniques biométriques sont le plus communément utilisées.

L'interopérabilité des systèmes des États membres de l'espace Schengen reste toutefois insuffisante et le projet « *frontières intelligentes* » devra gagner en ambition pour renforcer notre capacité à garantir une gestion rationnelle des frontières.

1. Un usage réel mais perfectible

a) La biométrie, un outil de base pour les gardes-frontières

De nombreux outils biométriques sont d'ores et déjà utilisés par les gardes-frontières pour s'assurer de l'identité des individus souhaitant entrer ou sortir de l'espace Schengen et pour fluidifier les files d'attente : **le système PARAFE, les passeports et visas biométriques, le dispositif EURODAC, *etc.***

Le contrôle à la frontière est organisé en **deux étapes** comme vos rapporteurs ont pu le constater lors de leur déplacement à la gare du Nord le 24 mars dernier.

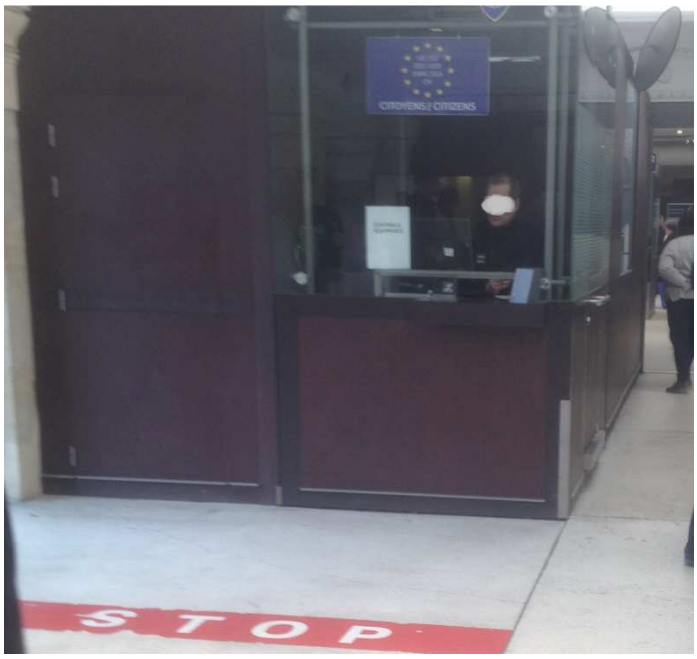
- ***Le contrôle de première ligne***

Ce contrôle est réalisé par un garde-frontière posté dans une aubette. Sa durée moyenne est estimée à **25 secondes**.

Son principal objectif est **l'authentification du voyageur**, le garde-frontière vérifiant la régularité du document d'identité ainsi que la correspondance entre la photographie de ce dernier et le voyageur qui s'est présenté au poste frontière.

L'interrogation des fichiers reliés aux outils biométriques (VISABIO, EURODAC, *etc*.) **est possible mais n'est pas systématique**.

Une aubette à la frontière franco-britannique de la garde du Nord[1]



Source : commission des lois du Sénat

- ***Le contrôle de seconde ligne***

Ce contrôle est réalisé **en cas de doutes sur l'identité de la personne**. Les garde-frontières procèdent à **l'identification** du voyageur : ses empreintes digitales sont prélevées pour être comparées aux données enregistrées dans les fichiers reliés aux outils biométriques.

Effectué dans un local séparé et spécialement prévu à cet effet, ce contrôle dure en moyenne 4 minutes.

b) Une interopérabilité encore limitée

Lors de leurs auditions, vos rapporteurs ont constaté avec étonnement le **faible niveau d'interopérabilité des dispositifs biométriques utilisés à l'échelle de l'espace Schengen**.

[1] *Photographie prise lors du déplacement de vos rapporteurs le 24 mars 2016.*

À titre d'exemple, les autorités françaises ne peuvent pas accéder aux empreintes digitales des **passeports** et des **documents de voyage** délivrés par les autres États de cet espace, ce qui réduit considérablement la qualité des contrôles.

Concrètement, les puces de ces titres comprennent **plusieurs** « ***couches*** » :

- une **première** lisible à partir d'une combinaison de chiffres présente sur le passeport (**code bande MRZ**) ;

- une **seconde qualifiée de « *BAC* » (« *basic access control* »)** contenant les informations relatives à l'identité du voyageur (nom, prénoms, date de naissance notamment) et sa photographie. Ces **données** sont **accessibles** à l'ensemble des États membres ;

- une **troisième désignée sous le terme de « *EAC* » (« *extended access control* »)** qui comprend les empreintes digitales du voyageur. Son **accès est beaucoup plus restreint** dans la mesure où il est protégé par un haut niveau de cryptographie.

Le règlement (CE) n° 2252/2004 du conseil du 13 décembre 2004[1] organise les conditions dans lesquelles les États peuvent s'échanger les informations contenues dans cette troisième couche. Il s'agit, concrètement, de **communiquer aux autres pays des certificats de sécurité.**

La Commission européenne a développé, pour ce faire, le **programme d'échange « *SPOC* » (« *single point of contact* »)**. Toutefois, à ce stade, ce dispositif n'est toujours pas effectif et ce pour plusieurs raisons.

Les États ont d'abord tardé à s'y investir. Constatant que la date limite de mise en œuvre du SPOC – 20 mai 2012 – n'avait pas été respectée, la Commission européenne a, par exemple, saisi la France le 13 mars 2013 avant de la mettre officiellement en demeure en janvier 2014.

Le déploiement du SPOC soulève également des **difficultés techniques importantes**.

Des problèmes d'interopérabilité ont ainsi été constatés lors des phases d'expérimentation, la phase de test de janvier 2015 menée par l'ANTS avec la République tchèque, la Hongrie, l'Irlande, l'Italie et la Roumanie n'ayant pas donné satisfaction. Cette interopérabilité est d'autant plus compliquée à assurer que les États membres modifient leurs certificats de sécurité plusieurs fois par an dans une logique de sécurisation des titres[2].

---

[1] *Règlement 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.*

[2] *Le certificat de sécurité des passeports français est par exemple modifié tous les trois mois.*

En dépit de ces difficultés d'ordre technique, vos rapporteurs considèrent qu'il est **urgent de rendre effectif l'échange de ces certificats de sécurité** afin d'accroître l'efficacité des outils à la disposition des gardes-frontières.

Proposition n° 5 : Relancer la procédure d'échange de certificats de sécurité entre les États membres de l'espace Schengen pour permettre à chacun d'eux d'accéder aux empreintes digitales enregistrées dans les passeports et les titres de voyage biométriques émis par des pays de l'espace Schengen.

D'une manière générale, il peut s'avérer opportun d'**harmoniser les dispositifs de recueil de données à l'échelle de l'Union européenne**, voire de **croiser certains fichiers nationaux** pour des besoins strictement définis.

Les garanties apportées aux citoyens devraient être renforcées dans cette hypothèse. Il conviendrait notamment de veiller à une bonne articulation entre la Commission nationale de l'informatique et des libertés (CNIL) et les autres autorités européennes de protection des données personnelles.

Proposition n° 6 : Offrir au niveau européen des garanties au moins identiques à celle données par la CNIL en France dès lors qu'il apparait indispensable d'harmoniser nos dispositifs de recueil de données dans les fichiers européens et de croiser certains de nos fichiers nationaux.

Veiller à ce que chaque développement et croisement de fichiers envisagé s'effectue dans un environnement respectant strictement la finalité des fichiers utilisés et le principe de proportionnalité.

2. Le projet « frontières intelligentes »

La Commission européenne a proposé, dès février 2008, de moderniser les méthodes de gestion des frontières extérieures de l'espace Schengen dans le cadre du projet intitulé *« frontières intelligentes »*[1]. Elle a également présenté des propositions législatives début 2016[2] avec un objectif de mise en œuvre concrète de ce dispositif à compter de 2020.

Les techniques biométriques jouent un rôle central dans ce programme, la Commission considérant qu'elles constituent un *« moyen fiable d'identifier les ressortissants de pays tiers qui se trouvent sur le territoire des États membres sans document de voyage ni aucun autre moyen d'identification »* et

[1] « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », *communication COM (2008) 69 du 13 février 2008 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:FR:HTML).*

[2] *Propositions de règlements européen COM (2016) 194 et COM (2016) 196 du 6 avril 2016 (http://ec.europa.eu/).*

qu'elles permettent « *un recoupement plus fiable des données relatives aux entrées et aux sorties des voyageurs en règle* »[1].

Les dispositifs utilisés mobiliseraient plusieurs types de biométrie avec une **priorité donnée à la reconnaissance faciale et, en cas de doutes, aux contrôles des empreintes digitales**[2].

Le projet « *frontières intelligentes* » comprend, concrètement, **deux dispositifs : le programme d'enregistrement des voyageurs (RTP), d'une part, et le système d'entrée/sortie (EES), d'autre part.**

a) Le programme d'enregistrement des voyageurs (RTP)

Le RTP que propose la Commission européenne est un **dispositif facultatif à l'attention des États membres souhaitant fluidifier le trafic des voyageurs**. Il s'inscrit ainsi dans **la même logique que le système français PARAFE** tout en ajoutant une technique biométrique complémentaire : la reconnaissance faciale.

Il s'agit de mettre à la disposition des voyageurs des systèmes d'identification en libre-service (**bornes**) et des portes électroniques (**sas**). Ces systèmes pourraient être :

- entièrement automatisés (une porte électronique s'ouvre après utilisation de la borne)[3] ;

- ou semi-automatisés (le voyageur s'identifie auprès de la borne mais est autorisé à franchir la frontière par un garde-frontière).

Un tel dispositif est en cours d'expérimentation à la gare de Saint-Pancras à Londres.

[1] *Proposition de règlement européen COM (2016) 194 précitée, p. 18-19.*

[2] *La commission propose le prélèvement des quatre empreintes digitales de l'index, du majeur, de l'annulaire et de l'auriculaire de la main droite.*

[3] *Ce dispositif ne serait pas accessible aux ressortissants de pays tiers de l'Union s'ils ne sont pas encore enregistrés dans le système d'entrée/sortie (EES), des recueils de données complémentaires étant nécessaires pour figurer dans ce dernier.*

Prototypes du programme d'enregistrement des voyageurs (gare de Saint-Pancras)

Source : Eurostar

La direction centrale de la police aux frontières (DCPAF) participe également aux **expérimentations relatives au programme d'enregistrement des voyageurs (RTP)**, tests que vos rapporteurs encouragent fortement dans l'optique de généraliser ces dispositifs à compter de 2020.

« *Frontières intelligentes* » : les expérimentations françaises

La DCPAF a procédé en 2015 à deux expérimentations de sas à reconnaissance faciale installés à la **gare du Nord** et à **l'aéroport Roissy-Charles de Gaulle**. Dans ce dernier cas, l'expérimentation comportait également l'inscription fictive des voyageurs dans une base de données type « *système d'entrée/sortie (EES)* » *(Cf. infra)*.

	Gare du Nord	**Aéroport Roissy-Charles de Gaulle**
Durée de l'expérimentation	Six semaines et demie	Huit semaines
Nombre de participants *(sur la base du volontariat)*	1 735	9 736
Taux de réussite de la reconnaissance faciale	91 %	86 %
Durée de la procédure *(temps pour franchir la frontière)*	22,6 secondes	30,2 secondes
Taux de satisfaction des participants	98 %	91 %
Intégration fictive dans un fichier type EES	Non	Oui

Source : commission des lois à partir des données de la DCPAF

Les taux d'échec de la reconnaissance faciale demeurent non négligeables pour une prise de photographie « *statique* » du voyageur[1]. En cas d'échec, l'intervention d'un garde-frontière est nécessaire pour permettre, ou non, le franchissement de la frontière.

La France a également testé une solution de **reconnaissance par l'iris à la gare maritime de Cherbourg**. Longue de treize semaines, cette expérimentation consistait à reconnaître à distance l'iris des passagers d'automobiles sans qu'ils ne quittent leur véhicule.

Cette technique a fonctionné pour 81 % des 3 400 participants à l'expérimentation. La durée de capture des iris (3,9 secondes) n'a pas rendu le trafic automobile plus difficile. Le taux de satisfaction des participants a atteint 91 % mais, d'après la DCPAF, ***« la capture de l'iris a été considérée comme l'option (biométrique) la plus intrusive de toute »***.

Alors que le programme d'enregistrement des voyageurs (RTP) ne concernait initialement que les **ressortissants de pays tiers** à l'espace Schengen, la Commission l'a étendu aux **citoyens européens** à l'occasion des propositions de règlement publiées le 6 avril 2016.

Les personnes entendues en audition par vos rapporteurs ont insisté sur le caractère positif de cette décision, le RTP devant être accessible à un nombre maximal de personnes pour répondre à l'objectif de fluidification du trafic.

b) Le système d'entrée/sortie (EES)

Second dispositif du programme « *frontière intelligente* », le système d'entrée/sortie (EES) serait une **base de données biométriques** permettant d'**enregistrer les passages à la frontière extérieure de l'espace Schengen des ressortissants de pays tiers**[2]. Son principal objectif est « *d'identifier tout migrant sans papiers en situation irrégulière, repéré sur le territoire après avoir légalement franchi les frontières extérieures* »[3].

Un **dossier individuel** serait créé pour chacun de ces ressortissants lorsqu'ils franchissent pour la première fois la frontière de l'espace Schengen. Ce dossier contiendrait des données relatives à leur état civil mais également leur image faciale et leurs empreintes digitales. Il serait complété par des ***« fiches »*** à chaque entrée et sortie indiquant la date et le lieu de ces mobilités. L'ensemble de ces données serait conservé pendant cinq ans dans une base de données créée à l'échelle européenne.

Le système d'entrée/sortie comporterait également une ***« calculatrice automatique »*** déterminant automatiquement le nombre de jours passés dans l'espace Schengen et alertant les États dans l'hypothèse où

---

[1] *Les taux d'échecs seraient, en outre, plus importants en cas de prise mobile (personne marchant dans une foule par exemple.*

[2] *Ce dispositif serait toutefois allégé pour les étrangers possédant un visa biométrique, leurs données étant conservées dans le système d'information sur les visas (VIS) et ce dernier étant, selon le projet de la Commission, relié au futur système d'entrée/sortie (EES).*

[3] *Proposition de règlement européen COM(2016) 194 précitée, p. 4.*

la période de séjour autorisée (90 jours par exemple pour un visa de court séjour) aurait expiré. L'EES indiquerait également les cas où l'entrée sur le territoire d'un pays de l'espace Schengen a été refusée ainsi que les motifs de ce refus.

La base correspondant au système EES serait **consultable à des fins répressives** dans des conditions comparables à celles applicables au système EURODAC. Il s'agit, d'après la Commission[1], « *d'aider à l'identification fiable des terroristes, des criminels ainsi que des suspects et des victimes* », notamment en fournissant « *un historique des déplacements des ressortissants de pays tiers, y compris ceux qui sont soupçonnés d'infractions graves* »[2].

Vos rapporteurs approuvent le déploiement du système d'entrée/sortie (EES) dans la mesure où il permettra une **gestion plus rationnelle des frontières extérieures de l'espace Schengen**.

Ils rejoignent toutefois la commission des affaires européennes du Sénat[3] pour solliciter l'extension de certaines dispositions du système EES aux citoyens européens ainsi qu'aux personnes vivant dans la zone Schengen et pas uniquement aux ressortissants d'États tiers. Il ne serait toutefois pas nécessaire, dans cette hypothèse, de prévoir un historique systématique de leur mobilité, les contrôles devant être concentrés sur des cas spécifiques.

Un tel dispositif faciliterait par exemple la mise en œuvre des interdictions de sortie du territoire prononcées lorsqu'il existe des raisons sérieuses de penser que la personne projette des déplacements à l'étranger ayant pour objet la participation à des activités terroristes[4].

Proposition n° 7 : Étendre le système d'entrée/sortie (EES) aux frontières de l'espace Schengen aux ressortissants communautaires, sans constitution, sauf situation spécifique, motivée et encadrée, d'historique des mouvements constatés.

[1] *Proposition de règlement européen COM(2016) 194 précitée, p. 5.*

[2] *La reconstitution de cet historique à des fins répressives ne serait possible que pour les crimes les plus graves (*Cf. *la première partie du rapport concernant l'interrogation du système EURODAC). Elle nécessiterait d'avoir déjà interrogé, sans succès, les bases de données nationales et d'avoir des* « motifs raisonnables de penser » *que la consultation de l'EES contribuera* « de manière significative » *à la résolution de l'affaire.*

[3] « L'Europe de Schengen face à la crise des réfugiés », *rapport d'information n° 499 (2015-2016) de MM. Jean-Yves Leconte et André Reichardt, fait au nom de la commission des affaires européennes, p. 23 (https://www.senat.fr/rap/r15-499/r15-4991.pdf).*

[4] *Article L. 224-1 du code de la sécurité intérieure.*

C. EXPÉRIMENTER LA CONNEXION ENTRE VIDÉOPROTECTION ET BASE DE DONNÉES

Les **nouvelles potentialités des techniques biométriques** ont été présentées à vos rapporteurs dans le cadre de leurs auditions et conduisent à s'interroger sur leur éventuelle mise en œuvre à moyen terme.

La **connexion entre les dispositifs de vidéoprotection et des bases de données** est sans doute la technologie posant le plus grand nombre de questions sur les plans éthique, technique et juridique.

Il s'agirait, concrètement, d'**identifier une personne en temps réel à partir d'un dispositif de reconnaissance faciale** après avoir relié un système de vidéoprotection, d'une part, et un fichier contenant les photographies d'individus recherchés, d'autre part.

1. Un questionnement juridique récurrent

Nos anciens collègues Jean-Patrick Courtois et Charles Gautier s'étaient montrés très **réservés** sur cette éventualité à l'occasion de leur **rapport d'information de décembre 2008 relatif à la vidéosurveillance**[1]. Ils écrivaient ainsi que « *cette perspective changerait considérablement la nature de l'outil (de vidéoprotection). Les craintes quant à une société de surveillance seraient considérablement ravivées et justifiées. On peut d'ailleurs se demander si ce type d'applications ne remettrait pas en cause l'acceptation de la vidéoprotection par les citoyens* ».

Ce même rapport de 2008 citait, en outre, M. Jean-Jacques Froment, professeur de droit public à la faculté de Grenoble, selon lequel la « *vidéoprotection intelligente* » présenterait de **« *nouveaux risques* »** : « *risque de stigmatisation discriminante de certaines catégories de population, émergence de nouvelles finalités, disproportion des moyens employés* ».

De même, comme le souligne la Commission nationale de l'informatique et des libertés (CNIL), la reconnaissance faciale « *fait peser des **risques importants sur les libertés individuelles** : le visage est (…) une donnée pouvant être captée à l'insu des personnes (…). Par ailleurs, le contexte actuel est caractérisé par une multiplication du nombre des systèmes de vidéoprotection, permettant en théorie le développement massif de la reconnaissance faciale* »[2].

Force est toutefois de constater que ce **débat est renouvelé par les avancées technologiques** observées et **le niveau élevé de menace auquel sont exposés nos concitoyens. Dans certains cas, cela impose aujourd'hui**

---

[1] *Rapport n° 131 (2008-2009) fait au nom de la commission des lois du Sénat, p. 13 et 46 (https://www.senat.fr/rap/r08-131/r08-1311.pdf).*

[2] *CNIL, 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 (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032372514).*

de longues files d'attente pour être contrôlé – files qui représentent parfois un risque en matière de sécurité – ou conduit parfois, au contraire, à une absence de contrôle faute de moyens humains. Si les techniques de « *vidéoprotection intelligente* » n'offrent pas un degré de fiabilité suffisant à ce jour, des expérimentations pourraient être menées dans un cadre juridique spécifique et restrictif permettant de tester les nouvelles possibilités offertes par la technologie.

2. Des incertitudes techniques persistantes

Les technologies de reconnaissance faciale « *statiques* » (prise de photographies devant une borne prévue à cet effet) ne sont pas les techniques biométriques les plus fiables. Les expérimentations « *frontières intelligentes* » menées à la gare du Nord et à l'aéroport Roissy-Charles de Gaulle le démontrent avec un taux de réussite compris entre 86 et 91 %[1], taux qui tombe d'ailleurs à 69 % dans l'expérience à la gare maritime de Cherbourg.

Les **taux d'erreurs des technologies « *dynamiques* »** (reconnaissance d'un individu dans une foule mobile) sont, en outre, largement supérieurs.

Entendue par vos rapporteurs, Mme Bernadette Dorizzi, professeure à l'école Telecom Sud-Paris, a émis de **sérieux doutes sur les potentialités des technologies dynamiques, y compris à moyen terme**. Il serait sans doute nécessaire de compléter la recherche en reconnaissance faciale par des indices autres que le visage[2].

Un **dispositif faisant le lien entre captation vidéo et fichiers** est opérationnel depuis 2007 pour le contrôle des véhicules mais il semble plus aisé à mettre en œuvre d'un point de vue technique.

Le système de lecture automatisée des plaques d'immatriculation (LAPI)

Prévu aux articles L. 233-1 et L. 233-2 du code de la sécurité intérieure, ce système permet aux forces de police et de gendarmerie de **lire automatiquement les plaques minéralogiques des véhicules** et de prendre une photographie de leurs occupants.

Ce dispositif peut être mis en œuvre dans tous les « *points appropriés* » du territoire (zones frontalières, axes routiers stratégiques, *etc.*) **pour un des motifs fixés par la loi** (infractions criminelles, vols de véhicules, lutte contre le terrorisme, lutte contre la criminalité organisée, maintien de l'ordre public lors de grands événements, *etc.*).

Les informations relatives aux plaques minéralogiques sont **automatiquement reliées au fichier des objets et des véhicules signalés (FOVeS) ainsi qu'au système d'information Schengen (SIS)**. Elles sont conservées dans des conditions strictement définies par le code de la sécurité intérieure :

[1] Cf. *supra.*
[2] *Manière dont la personne recherchée est habillée notamment.*

- les données n'ayant pas fait l'objet d'un rapprochement positif avec les bases de données précitées sont conservées pendant quinze jours[1] et ne sont pas consultables, sauf *« pour les besoins d'une procédure pénale ou douanière »* ;

- celles ayant fait l'objet d'un rapprochement positif sont enregistrées pendant un mois.

En 2014, 47 millions de plaques d'immatriculation ont été lues par les dispositifs LAPI de la gendarmerie nationale. 7 900 d'entre elles ont fait l'objet d'un rapprochement avec les bases FOVeS et SIS précitées, ce qui a permis la découverte de 600 véhicules volés.

L'article 15 *bis* B du projet de loi portant application des mesures relatives à la justice du XXIe siècle prévoit, enfin, une extension du LAPI aux systèmes de diagnostic embarqués, dans le cadre du contrôle des dispositions techniques liées aux véhicules.

Rappelons, en outre, que **les photographies insérées dans le fichier de traitement des antécédents judiciaires (TAJ)** comportent déjà *« des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale (photographie du visage de face) »*[2], dispositif que le Conseil d'État a jugé *« adéquat, pertinent et non excessif par rapport à (ses) finalités »*[3].

Une circulaire d'application précise ainsi que *« l'objectif poursuivi est de procéder à des rapprochements entre les photographies contenues dans le TAJ et, par exemple, un visage apparaissant sur des images enregistrées par une caméra de vidéo-protection »*[4].

Ce dispositif est toutefois plus circonscrit que le système de reconnaissance faciale examiné par le présent rapport dans la mesure où :

- **il ne s'agit pas d'un dispositif de reconnaissance en temps réel**, les images des caméras de vidéoprotection étant analysées *a posteriori* ;

- **son usage est limité** aux procédures de recherche des causes de la mort ou d'une disparition ainsi qu'aux enquêtes préliminaires ou de flagrance et aux investigations exécutées sur commission rogatoire, dans l'hypothèse où elles concernent un trouble à la sécurité ou à la tranquillité publiques ou une atteinte aux personnes, aux biens ou à l'autorité de l'État[5].

---

[1] *Ce délai était initialement de huit jours mais il a été allongé par l'article 104 de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.*

[2] *Article R. 40-26 du code de procédure pénale.*

[3] *Conseil d'État,* Ligue des droits de l'homme, *11 avril 2014, n° 360759.*

[4] *Circulaire du Garde des Sceaux du 18 août 2014 et relative aux fichiers d'antécédents judiciaires (http://www.textes.justice.gouv.fr/art_pix/JUSD1419980C.pdf)*

[5] *Article 230-6 du code de procédure pénale.*

3. Le nécessaire encadrement juridique d'éventuelles expérimentations

Le contexte actuel conduit toutefois vos rapporteurs à **ne pas sous-estimer l'apport potentiel d'une connexion entre des systèmes de vidéoprotection et des bases de données** ainsi que la **nécessité d'engager un processus d'expérimentation en la matière.**

Cette expérimentation n'est envisageable que dans la mesure où des **garanties substantielles** sont prévues pour assurer un équilibre entre prévention et répression des troubles à **l'ordre public, d'une part, et respect du droit à la vie privée des personnes, d'autre part**. En effet, comme le rappelle le Conseil constitutionnel, « *la prévention d'atteintes à l'ordre public (…) sont nécessaires à la sauvegarde de principes et droits à valeur constitutionnelle. (Il) appartient au législateur d'assurer la conciliation entre ces objectifs de valeur constitutionnelle et l'exercice des libertés publiques constitutionnellement garanties au nombre desquelles figurent la liberté individuelle et la liberté d'aller et venir ainsi que l'inviolabilité du domicile. (La) méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* »[1].

En tout état de cause, connecter des systèmes de vidéoprotection à des bases de données **nécessiterait de respecter à la fois** :

- **le droit applicable à l'installation de caméras** captant des images sur la voie publique, dans les lieux et établissements ouverts au public ou aux abords immédiats des bâtiments et installations de personnes morales de droit privé (articles L. 251-1 à L. 255-1 et L. 222-1 à L. 223-9 du code de la sécurité intérieure) ;

- **les règles applicables à la protection des données personnelles (**loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

Les garanties à prévoir concernent les autorités qui seraient en charge de la gestion d'un tel dispositif, les finalités poursuivies, les traitements de données concernés, la durée de conservation des informations ainsi que l'organisation de différents contrôles.

- ***Les personnes ayant accès au dispositif : des autorités publiques***

Le régime général applicable à la vidéoprotection distingue deux cas de figure concernant l'enregistrement des images. Cette procédure peut être assurée par :

- des autorités publiques : services de police et de gendarmerie nationales ainsi que des douanes et des services d'incendie et de secours ;

[1] *Décision n° 94-352 DC du 18 janvier 1995,* Loi d'orientation et de programmation relative à la sécurité.

- les personnels de sociétés privées dans l'hypothèse où la zone couverte par le dispositif de vidéoprotection est ouverte au public et exposée à un risque terroriste[1]. Le Conseil constitutionnel a précisé en 2011[2] que cette compétence ne peut être étendue à la surveillance de la voie publique car cela relève des « *missions de souveraineté* » de l'État qui ne peuvent être déléguées à une personne privée au regard de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789[3].

Cette jurisprudence du Conseil constitutionnel paraît transposable à l'éventuelle connexion entre un dispositif de vidéoprotection et des bases de données. La tenue de ces fichiers étant à la charge de l'État et les données contenues étant sensibles, **seuls des agents individuellement désignés et dûment habilités des services de police et de gendarmerie pourraient exploiter un tel dispositif.**

• ***Les finalités : une priorité à donner à la prévention et la lutte contre le terrorisme***

Expérimenter une liaison entre un dispositif de vidéoprotection et une base de données suppose également de préciser les finalités de cette démarche.

Les finalités des traitements de données à caractère administratif ou judiciaire[4] ou celles de la vidéoprotection ne sont pas transposables en l'état dans la mesure où elles apparaissent trop larges pour répondre au principe de proportionnalité fixé par le Conseil constitutionnel.

Les neuf finalités de la vidéoprotection
(Article L. 251-2 du code de la sécurité intérieure)

1° La protection des bâtiments et installations publics et de leurs abords ;

2° La sauvegarde des installations utiles à la défense nationale ;

3° La régulation des flux de transport ;

4° La constatation des infractions aux règles de la circulation ;

5° La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le second alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions ;

6° La prévention d'actes de terrorisme (…) ;

[1] *Article L. 223-1 du code de la sécurité intérieure.*
[2] *Décision n° 2011-625 DC du 10 mars 2011,* Loi d'orientation et de programmation pour la performance de la sécurité intérieure.
[3] *Article disposant que* « la garantie des droits de l'homme et du citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée ».
[4] Cf. *la première partie du présent rapport.*

7° La prévention des risques naturels ou technologiques ;

8° Le secours aux personnes et la défense contre l'incendie ;

9° La sécurité des installations accueillant du public dans les parcs d'attraction.

Vos rapporteurs considèrent que la priorité doit être donnée à **la prévention et la lutte contre les actes terroristes tels que définis aux articles 421-1 et suivants du code pénal** et non à d'autres finalités qui pourraient nuire à l'efficacité du dispositif ou s'avérer disproportionnées.

Il conviendrait également de **prendre garde à toute extension des finalités** d'une liaison entre vidéoprotection et bases de données afin d'éviter une dynamique d'extension du champ couvert par le dispositif, dynamique notamment constatée dans le cas du fichier national automatisé des empreintes génétiques (FNAEG)[1].

- ***Les modalités de mise en œuvre : la création d'un nouveau fichier***

Un tel dispositif nécessiterait, en outre, de fixer des modalités d'exécution très strictes. Par analogie avec le cadre applicable à la vidéoprotection, les forces de l'ordre devraient renseigner un **registre** mentionnant les enregistrements réalisés et les personnes concernées[2]. Le **public devrait également être informé** « ***de manière claire et permanente*** *de l'existence (de la liaison caméras/ base de données) et de l'autorité ou de la personne responsable* »[3].

À ce stade, il semblerait qu'aucun fichier existant ne pourrait être directement relié à un dispositif de vidéoprotection dans la mesure où se posent :

a) un **problème d'ordre technique**, les photographies contenues dans les fichiers existants n'ayant pas été prises dans un cadre normalisé permettant leur rapprochement avec une image de vidéoprotection.

Certains fichiers ne comportent, en outre, aucune photographie des personnes concernées à l'instar du fichier judiciaire national automatisé des auteurs d'infractions terroristes. D'autres, comme le fichier des personnes recherchées, ne comprennent pas des éléments visuels pour chaque personne recensée. Les coûts d'ajustement techniques pourraient donc s'avérer importants, voire dirimants.

D'un point de vue technique, les auditions de vos rapporteurs ont également démontré qu'une reconnaissance faciale instantanée implique **une base de données restreinte comprenant, au maximum, 100 000 à 500 000 personnes**. **Accroître de manière excessive le nombre d'individus recensés dans le fichier pourrait ainsi ralentir le fonctionnement du**

[1] Cf. *la première partie du présent rapport.*
[2] *Article R. 252-11 du code de la sécurité intérieure.*
[3] *Article L. 251-3 du code de la sécurité intérieure.*

dispositif – ce dernier devant alors croiser un nombre croissant de données – **et donc nuire à son efficacité.**

b) un **problème juridique**, les fichiers existants ayant des finalités trop larges ou s'inscrivant dans des procédures judiciaires spécifiques.

L'inadaptation des fichiers existants : quelques exemples

- Fichiers aux finalités trop larges

Quinze motifs justifient l'inscription au **fichier des personnes recherchées (FPR)**, dont la plupart ne semble pas justifier une connexion avec un système de vidéoprotection : interdictions de stade, interdiction de conduire certains véhicules terrestres à moteur, personnes considérées comme insoumises ou déserteurs en application des dispositions des articles 397 à 404 du code de justice militaire, *etc*[1].

De même, le **fichier automatisé des empreintes digitales (FAED)** comporte les données de personnes suspectées ou reconnues coupables d'infractions de recel ou de blanchiment, de trafic de stupéfiants, *etc*[2].

- Fichier s'inscrivant dans des procédures judiciaires spécifiques

Créé par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, le **fichier judiciaire national automatisé des auteurs d'infractions terroristes** se borne à contenir des informations relatives à des personnes condamnées ou mises en examen et pour lesquelles le juge d'instruction a ordonné une inscription au fichier.

Il semble donc nécessaire de créer un nouveau fichier dont le champ et les caractéristiques techniques seraient spécialement dédiés à un système de connexion avec des caméras de vidéoprotection.

• ***La modalité de conservation des données : s'inspirer du système de lecture automatisée des plaques d'immatriculation***

Des **conditions strictes de conservation des données** devraient être prévues concernant l'éventuelle connexion entre des dispositifs de vidéoprotection et des bases de données. Ces données seraient en effet très sensibles dans la mesure où elles seraient recueillies sans l'accord exprès des personnes.

Il semble possible de s'inspirer du système de lecture automatisée des plaques d'immatriculation (LAPI)[3] en prévoyant :

- un délai de quelques jours pendant lequel sont conservées les images de vidéoprotection n'ayant pas donné lieu à un rapprochement positif avec une base de données. Leurs consultations ne seraient alors pas possibles, sauf pour les besoins d'une procédure pénale relative à un acte terroriste ;

[1] *Article 230-19 du code de procédure pénale.*
[2] *Article 706-55 du code de procédure pénale.*
[3] Cf. *supra.*

- un délai de conservation un peu plus étendu pour les images ayant fait l'objet d'un tel rapprochement[1].

• ***Les contrôles : prévoir l'intervention de la CNIL ainsi qu'une durée d'expérimentation limitée***

La Commission nationale de l'informatique et des libertés (CNIL) serait compétente dans le cadre de cette expérimentation puisque cette dernière utilise un traitement automatisé permettant d'identifier, directement ou indirectement, des personnes physiques[2].

Ce dispositif serait créé par décret en Conseil d'État après avis consultatif de la CNIL, conformément au droit en vigueur[3].

Il conviendrait, également, de **circonscrire la durée de l'expérimentation**. Si les systèmes de vidéoprotection classiques sont autorisés pour cinq ans renouvelables, la durée pendant laquelle la présente expérimentation serait permise ne devrait pas dépasser **un an**.

Proposition n° 8 : Accepter une expérimentation de la reconnaissance faciale reliant les systèmes de vidéoprotection à des fichiers de « *personnes à risque* », l'objectif étant de disposer de nouveaux outils pour prévenir et réprimer les actes terroristes dans des conditions de forte affluence qui limitent, et parfois rendent même dangereux, le recours à des fouilles ou à des contrôles systématiques.

Prévoir des garanties spécifiques, notamment en :

- s'inspirant, en plus restrictif, des modalités de conservation des données du système de lecture automatisée des plaques d'immatriculation (LAPI) ;

- prévoyant une durée d'expérimentation limitée à un an.

[1] *Cette durée serait ainsi identique au délai de conservation des images de vidéoprotection prévu par l'article L. 252-3 du code de la sécurité intérieure.*

[2] *Article L. 251-1 du code de la sécurité intérieure et avis n° 385.125 du 24 mai 2011 de la section de l'intérieur du Conseil d'État.*

[3] Cf. *la première partie du présent rapport.*

CONCLUSION

Le développement de la biométrie constitue une **opportunité pour les pouvoirs publics** en termes de sécurisation de l'identité des individus et de rationalisation de l'action administrative.

Les outils biométriques – dont la puissance dépend de la progression de la puissance de calcul des dispositifs informatiques, des capacités de stockage et d'échanges d'informations – soulèvent cependant des **questions techniques** (fiabilité des dispositifs) **et juridiques** (équilibre à atteindre avec le droit au respect de la vie privée).

Ils présentent également un enjeu important de **souveraineté numérique** et de **politique industrielle**.

Les **entreprises françaises** ont en effet développé un savoir-faire reconnu au niveau mondial et fournissent les États en solutions de sécurité biométrique.

Il convient donc de demeurer attentif au cadre juridique qui leur est applicable afin qu'elles puissent maintenir leurs capacités de recherche et développement en France. En effet, ce cadre juridique doit assurer aux entreprises leur capacité d'innovation, tout en ne tolérant aucune dérive sur le plan des principes, notamment en matière de traitement de données.

Nos entreprises doivent être reconnues comme innovantes mais également garantir des dispositifs protecteurs de l'intégrité des personnes.

Proposition n° 9 : Tout en ne perdant pas de vue que la biométrie n'est pas infaillible et qu'il convient d'en comprendre les limites, disposer de conditions économiques et juridiques permettant de préserver et renforcer les capacités françaises de recherche et développement afin de conserver la maîtrise de l'élément de souveraineté que représentent les outils biométriques.

EXAMEN EN COMMISSION

_____

MERCREDI 13 JUILLET 2016

M. Philippe Bas, président. – MM. Leconte et Bonhomme vont nous présenter un rapport d'information sur la biométrie.

M. Jean-Yves Leconte, rapporteur. – Nous travaillons sur ce rapport depuis un peu plus d'un an. Le sujet n'est d'ailleurs pas nouveau ; ainsi M. Gaëtan Gorce avait déposé une proposition de loi sur la biométrie en 2014.

La biométrie recouvre l'ensemble des technologies qui permettent d'identifier une personne, sur la base de son comportement ou de ses caractéristiques physiques.

En 2014, à l'occasion de l'examen de la proposition de loi de M. Gaëtan Gorce, nous avions conclu à la nécessité de réserver l'usage de la biométrie dans le domaine privé à des situations très sensibles comme la protection de l'intégrité physique ou de certaines informations. Dans ce rapport, nous avons examiné les usages publics (administratifs et judiciaires) de la biométrie en France et en Europe. Nous nous sommes demandé comment lutter contre le terrorisme tout en protégeant les libertés.

La biométrie donne le sentiment d'exister depuis la fin du XIX^{e} siècle avec les empreintes digitales. En réalité, le potentiel de ces techniques a beaucoup évolué. Il faut ajouter aujourd'hui la reconnaissance faciale, de l'iris de l'œil, de la voix et des contours de la main.

Les recherches actuelles s'orientent surtout vers les capacités de stockage, de calcul et d'échanges de données. En France, dans les années 1880, le travail de M. Alphonse Bertillon a permis d'accélérer les enquêtes, mais cet usage judiciaire a évolué vers un usage administratif, notamment à partir de 1912 pour identifier les nomades. Au cours du XX^{e} siècle, l'usage administratif de la biométrie a entraîné de nombreuses dérives. Avec les nouvelles techniques, il convient de prévoir un strict cadrage juridique, tant en ce qui concerne la finalité des fichiers biométriques que de la proportionnalité de leur utilisation et de la durée de conservation des données.

À partir des années 1980, de nouveaux fichiers biométriques ont vu le jour : il y a eu le fichier automatisé des empreintes digitales (Faed) en 1987. Aujourd'hui, cinq millions d'empreintes y sont enregistrées pour une durée de conservation de 25 ans maximum. Le fichier national des empreintes génétiques (Fnaeg) a été créé en 1998 et comprend 2,6 millions d'empreintes pour une durée maximum de 40 ans. Aujourd'hui, environ

300 fonctionnaires ont accès à ces fichiers et, en 2014, près de 15 000 affaires ont été résolues grâce au Faed.

Depuis le milieu des années 2000, en particulier sous l'impulsion des États-Unis après les attentats du 11 septembre, les passeports biométriques se sont développés. Ils permettent à leurs possesseurs d'entrer sur le sol américain sans visas. La norme de l'Organisation de l'aviation civile internationale (OACI) s'est imposée. Les usages administratifs de la biométrie ont alors commencé à se développer. L'Union européenne a élaboré le règlement de 2004 et la France a mis en place le fichier des titres électroniques sécurisés pour les passeports. Aujourd'hui, la France compte près de 23 millions de passeports biométriques, et le flux mensuel est d'environ 300 000 passeports délivrés.

Ces passeports sont constitués de trois niveaux d'informations contenues dans leur puce. Le premier niveau se trouve sur la bande électronique du passeport et concerne l'identité du détenteur. Le niveau « BAC » contient l'identité et la photo. Le niveau « EAC » comprend, en outre, les empreintes digitales. Alors que tous les passeports européens sont biométriques et répondent aux mêmes normes, la police de l'air et des frontières française n'a pas accès au niveau « EAC » d'un passeport allemand et réciproquement : les États ne se font pas suffisamment confiance pour donner les clés du niveau le plus élevé, en dépit des dires officiels de Bruxelles.

J'en viens aux autres fichiers biométriques : le fichier des visas a ainsi été mis en place en 2007 et généralisé à partir de 2015. La France a commencé par délivrer des visas biométriques pour la Géorgie et la Biélorussie, pays de petite taille. Dès lors qu'un visa biométrique est nécessaire, il faut que le demandeur vienne au bureau de délivrance du document pour une prise d'empreintes, ce qui était difficile à mettre en œuvre dans de grands pays comme la Russie. Depuis l'an passé, ces visas biométriques ont été généralisés dans tous les pays de l'espace Schengen. Aujourd'hui, les visas sont exclusivement biométriques. Pour la Russie par exemple, nous avons dû externaliser les bureaux où les empreintes sont prises. Ainsi, nul besoin d'avoir un consulat général dans toutes les grandes villes du pays : un prestataire de service assume ce travail pour notre pays mais aussi pour d'autres. En revanche, comme les pays ne se font pas suffisamment confiance, les clés pour entrer dans le système des visas européens sont différentes selon les États. Les prestataires doivent ainsi disposer de machines différentes selon que le visa est demandé pour aller en France ou en Espagne.

Le système Eurodac est utilisé pour enregistrer les personnes en situation irrégulière et les demandeurs d'asile afin d'éviter de multiples demandes des différents pays.

Le fichier Agdref concerne les demandeurs des cartes de séjour et les personnes sous le coup d'une obligation de quitter le territoire français (OQTF).

La biométrie permet donc de nouvelles formes d'identification, tout en luttant contre la fraude et en sécurisant les documents. L'émission « Cash investigation » de France Télévisions a néanmoins démontré que la fraude était toujours possible. 5 910 fausses cartes d'identité ont été découvertes en 2014 par les services de police et de gendarmerie…

En 2011, une proposition loi de notre ancien collègue Jean-René Lecerf avait envisagé de créer une carte nationale d'identité biométrique mais le Conseil constitutionnel l'avait en partie censurée car l'Assemblée nationale avait voulu un fichier à « lien fort » entre identité et empreintes, contrairement au Sénat qui, pour protéger les libertés individuelles, privilégiait le « lien faible » qui interdit l'identification d'une personne par ses seules empreintes. Il serait temps de rouvrir ce dossier en tenant compte des observations du Conseil constitutionnel.

La biométrie ne pourra pas empêcher toute usurpation d'identité, notamment en raison de fraudes lors de la première collecte des données corporelles ou comportementales.

En outre, les évolutions technologiques permettent désormais diverses interconnections, mais les différents systèmes utilisés dans divers pays entravent cette évolution. L'encadrement européen est indispensable pour éviter des atteintes aux libertés individuelles.

Ces nouvelles technologies offrent d'immenses possibilités mais comportent également de grands risques. La France compte des entreprises de premier plan en ce domaine : la maîtrise de ces technologies constitue un acte de souveraineté. Notre encadrement juridique devra respecter les libertés individuelles mais aussi permettre aux entreprises françaises de conserver leur prééminence. En cas contraire, nous assisterions à une perte de souveraineté et nous devrions nous en remettre à des technologies développées par d'autres pays.

M. François Bonhomme, rapporteur. – Les techniques biométriques permettent de sécuriser l'identité des personnes et d'accroître l'efficacité de l'action administrative comme M. Leconte vient de le démontrer. La spécificité des données biométriques a toutefois justifié l'émergence d'un cadre juridique particulier. En effet, les « données biométriques ne sont pas des données à caractère personnel comme les autres » pour reprendre les mots de la Commission nationale de l'informatique et des libertés (CNIL). Produites par le corps humain, elles font partie de l'intime de chacun.

Le droit aborde les données biométriques à partir d'une logique de proportionnalité : leurs apports pour l'intérêt général sont comparés aux effets de ces techniques sur la vie privée des individus. À l'échelle nationale, les outils biométriques sont encadrés par l'article 27 de la loi de 1978 relative

à l'informatique, aux fichiers et aux libertés : ils doivent être autorisés par décret en Conseil d'État pris après avis motivé et public de la CNIL. Cette dernière procède également à des vérifications *a posteriori* comme lorsqu'elle a contrôlé le fichier des passeports biométriques en 2012.

Au niveau constitutionnel, les sages de la rue de Montpensier ont développé une grille d'analyse permettant de vérifier la proportionnalité des techniques biométriques. Ainsi, le fichier national des empreintes génétiques (Fnaeg) a été jugé conforme à la Constitution dans la mesure où sa finalité est suffisamment précise et répond à l'objectif d'intérêt général de faciliter la recherche des auteurs de certaines infractions.

Tel n'a pas été le cas de certaines dispositions de la loi du 27 mars 2012 relative à la protection de l'identité comme l'a signalé M. Leconte. Cette loi prévoyait de créer une carte d'identité biométrique et un fichier central regroupant les informations correspondantes. Si le Conseil constitutionnel n'a pas contesté la carte d'identité biométrique en elle-même, il a censuré la création du fichier en estimant que les garanties apportées n'étaient pas suffisantes. À l'époque, notre collègue François Pillet avait proposé que cette base de données soit constituée à partir de « liens faibles » : un nombre élevé d'identités aurait été relié aux données biométriques correspondantes, ce qui aurait rendu les procédures d'identification plus compliquées voire impossibles. L'Assemblée n'a pas souhaité suivre cette position de prudence, ce qui a conduit le Conseil constitutionnel à censurer ce fichier.

Il convient, enfin, de ne pas sous-estimer les risques d'erreurs et de fraudes lors de l'utilisation d'outils biométriques. Le risque d'erreur est mesuré à partir de deux variables : le taux de fausses acceptations (le système n'arrive à pas à reconnaître un imposteur et à le rejeter) et le taux de faux rejets (le système rejette à tort une personne éligible). Ces deux taux sont interdépendants : si vous augmentez le niveau de sécurité de l'outil biométrique, vous reconnaîtrez plus d'imposteurs mais vous rejetterez plus de personnes éligibles. Les systèmes biométriques totalement infaillibles n'existent donc pas. En outre, le corps de chacun d'entre nous évolue : un système de reconnaissance faciale ne peut reconnaître un visage si la photographie date de plus de trente ans.

Outre les risques d'erreurs, les tentatives de fraudes ne sont pas à exclure. Les journalistes de l'émission « Cash investigation » de France Télévisions l'ont démontré en utilisant un « faux doigt » pour tromper les capteurs digitaux des sas PARAFE de Roissy.

Il est toutefois possible de mieux utiliser les dispositifs biométriques tout en ayant conscience de leurs limites et en préservant le droit à la vie privée de chacun. Il s'agirait, tout d'abord, d'utiliser la biométrie pour simplifier les relations entre les citoyens et leur administration. À cet égard, nous regrettons que les Français ne disposent pas encore d'une identité numérique fiable. En effet, le Gouvernement n'a pas souhaité mettre en

œuvre la loi de 2012 relative à la protection de l'identité et n'envisage pas de créer des cartes d'identité biométriques. L'Agence nationale des titres sécurisés (ANTS) développe un programme alternatif : le projet ALICEM qui permet aux citoyens d'utiliser leur passeport biométrique pour certifier leur identité à partir de leur téléphone portable et ainsi accéder à des services administratifs ou commerciaux en ligne. Il s'agit, pour l'instant, d'un prototype que nous appelons à généraliser dans notre première proposition.

Toutefois, ces différentes initiatives du Gouvernement ne peuvent se substituer à la création d'une carte d'identité biométrique que nous appelons de nos vœux dans notre deuxième proposition. Dans son rapport de 2016, la Cour des comptes souhaite également sa mise en œuvre. La position du législateur de 2012 n'a pas perdu en acuité, la biométrie constituant un moyen fiable pour lutter contre les fraudes documentaires. En outre, le passeport biométrique ne soulève aucune difficulté en termes d'acceptation sociale. Pourquoi en serait-il autrement pour les cartes d'identité ? D'ailleurs, beaucoup de pays de l'Union européenne possèdent déjà des cartes d'identité biométriques comme les Pays-Bas, l'Espagne ou la Lituanie.

De plus, la carte d'identité que nous possédons aujourd'hui et ses conditions de délivrance sont totalement obsolètes. Les empreintes digitales prélevées en mairie ne sont pas traitées informatiquement et ne sont donc pas exploitées. De même, la base de données relative aux cartes d'identité est peu fonctionnelle et doit être rénovée : profitons-en pour revoir tout le système et créer des cartes d'identité biométriques. Le coût d'un tel projet – environ 85 millions – ne paraît d'ailleurs pas excessif au regard des enjeux.

Nous nous sommes attachés à proposer un projet réaliste et conforme aux exigences du Conseil constitutionnel : une base de données serait créée à partir des cartes d'identité biométriques mais les liens seraient faibles pour rendre l'identification des personnes à partir de leurs empreintes plus difficile.

M. Jean-Yves Leconte, rapporteur. – Dans notre proposition n° 4, nous considérons qu'il est nécessaire de poursuivre la modernisation des procédures de délivrance des passeports et des visas biométriques : comme les empreintes ne se modifient pas en fonction de l'âge, il n'est pas nécessaire d'en demander un nouveau recueil lors d'un renouvellement de passeport biométrique. Nous éviterions ainsi la présentation physique de demandeurs aux guichets.

Il faut également approfondir la politique de mutualisation de la collecte des données biométriques des visas et l'étendre aux passeports. Il convient de prévoir l'envoi sécurisé des passeports pour les Français qui vivent hors de France mais aussi pour ceux qui vivent dans notre pays.

J'en reviens à la proposition n° 3. Des certificats de nationalité française (CNF) sont délivrés à des personnes qui viennent d'être naturalisées, ce qui peut poser problème lorsque les documents étrangers

servant à l'établissement du CNF ne sont pas fiables. Nous proposons que ces CNF puissent être reliés au fichier des passeports pour lutter contre la fraude documentaire.

La proposition n° 5 prévoit de relancer la procédure d'échange de certificats de sécurité entre les États membres de l'espace Schengen pour permettre à chacun d'eux d'accéder aux empreintes digitales enregistrées dans les passeports et les titres de voyage biométriques émis par des pays de l'espace Schengen. Il n'est pas normal que nous ne soyons pas en mesure de « lire » les passeports des autres États !

La proposition n° 6 consiste à offrir au niveau européen des garanties au moins équivalentes à celles données par la CNIL en France dès lors qu'il apparait indispensable d'harmoniser nos dispositifs de recueil de données dans les fichiers européens et de croiser certains de nos fichiers nationaux. Il convient également de veiller à ce que chaque développement et croisement de fichiers envisagé s'effectue dans un environnement respectant strictement la finalité des fichiers utilisés et le principe de proportionnalité.

Enfin, notre proposition n° 7 propose d'étendre le système d'entrée/sortie (EES) aux frontières de l'espace Schengen aux ressortissants communautaires, sans constitution, sauf situation spécifique, motivée et encadrée, d'historique des mouvements constatés. À l'entrée et à la sortie de l'espace Schengen, les voyageurs devraient être contrôlés systématiquement de façon biométrique, ce qui permettrait de valider les pièces d'identité, contrairement à la situation actuelle.

M. François Bonhomme, rapporteur. – J'en viens maintenant aux dernières propositions de notre rapport : nous proposons d'expérimenter les dispositifs de reconnaissance faciale reliant les systèmes de vidéo-protection à des fichiers. Concrètement, si une personne recherchée est filmée par des caméras de vidéo-protection reliées à une base de données, le système informatique enverrait une alerte aux forces de l'ordre pour les informer de la présence sur zone de cet individu. S'ils sont bien encadrés, de tels dispositifs permettraient de rendre plus efficace la prévention et la répression des actes de terrorisme en localisant plus facilement les personnes concernées. Lors de nos auditions, nous avons constaté que ce type de dispositifs se développait. Méfions-nous de tout « totem technologique », mais ces pistes doivent être explorées. À ce stade, ces dispositifs présentent encore des incertitudes techniques : les reconnaissances faciales statiques (prise de photographies devant une borne prévue à cet effet) ont un taux de réussite compris entre 70 et 90 %. Les systèmes de reconnaissance dynamique (reconnaissance du visage d'une personne se déplaçant dans une foule) ont un taux d'erreurs encore supérieur.

Il ne s'agit pas, non plus, de nier les questionnements juridiques soulevés par l'éventuelle connexion entre la vidéo-protection et des fichiers.

En 2008, nos anciens collègues Jean-Patrick Courtois et Charles Gautier s'étaient montrés très réservés sur cette hypothèse. Force est pourtant de constater que le débat est renouvelé par le niveau de menace auquel sont exposés nos concitoyens. En outre, notre proposition n° 8 n'est pas d'installer ce type de dispositifs dès maintenant mais de l'expérimenter et de réfléchir à un cadre juridique spécifique afin de pouvoir l'utiliser lorsque les techniques correspondantes seront plus fiables. Ainsi, connecter la vidéo-protection à des fichiers pour permettre des reconnaissances faciales supposerait le respect du droit applicable à l'installation de caméras et des règles de protection de données personnelles. Conformément à la jurisprudence du Conseil constitutionnel, seules des autorités publiques assermentées pourraient exploiter ce type de dispositifs.

Ces derniers devraient être utilisés pour une finalité suffisamment précise : nous proposons ainsi de limiter ces expérimentations à la prévention et à la répression des actes de terrorisme.

Lors de nos travaux, nous n'avons pas trouvé de fichiers qui pourraient être directement branchés à un système de vidéo-protection. Les fichiers existants sont soit trop larges, soit inadaptés d'un point de vue technique. Il conviendrait donc de créer un fichier spécifique puis de le mettre en relation avec des caméras. D'ailleurs, un système comparable existe déjà pour contrôler les plaques d'immatriculation des véhicules : il s'agit du système de lecture automatisée des plaques (LAPI). Il serait possible de s'en inspirer pour les modalités de conservation des données relatives à la reconnaissance faciale.

En conclusion, la biométrie constitue une opportunité pour les pouvoirs publics. Elle soulève toutefois des questions techniques et juridiques. La biométrie présente également un enjeu économique important de souveraineté numérique et de politique industrielle. Les entreprises françaises ont en effet développé un savoir-faire reconnu au niveau mondial et fournissent les États en solutions de sécurité biométrique. Une entreprise est ainsi intervenu en Inde sur un programme d'identification portant sur plus d'un milliard d'identités numériques, ce qui considérable.

Il convient donc de demeurer attentif au cadre juridique qui est applicable aux techniques biométriques afin qu'elles puissent maintenir leurs capacités de recherche et développement en France, ce qui est l'objet de notre neuvième et dernière proposition.

M. Philippe Bas, président. – Je vous remercie pour la qualité de vos travaux sur ces questions complexes qui traitent de la libre circulation et de la sécurité en Europe.

M. François Pillet. – Merci à nos rapporteurs pour l'excellence de leur travail. Le droit n'interdira pas l'usage de la biométrie ni l'évolution des connaissances. L'analyse des traces biométriques que nous laissons va continuer à progresser. Puisqu'on ne peut contenir l'usage de la biométrie,

celle-ci doit être encadrée. Le contrôle du stockage des données est donc essentiel : le Sénat devra s'ériger en sentinelle pour éviter la violation des libertés. Imaginez que le fichier des cartes d'identité biométriques prévu en 2012 soit utilisé par un pouvoir peu démocratique….

Lorsque nous avons étudié la proposition de loi de M. Lecerf, la majorité du Sénat était identique à celle de l'Assemblée nationale. Pour autant, nous n'avons pas accepté le fichier à « lien fort » prévu, estimant qu'il s'agissait d'une atteinte grave aux libertés et donc aux principes constitutionnels. D'ailleurs, le Conseil constitutionnel a repris quasiment les termes de nos débats. Pour autant, nous avons bien un problème de protection de l'identité nationale mais, alors que le Conseil constitutionnel n'avait annulé que le fichier, le Gouvernement n'a pas donné suite à la création d'une carte d'identité biométrique, ce qui tend à prouver que son objectif était de créer un fichier policier plutôt que d'améliorer les dispositifs de sécurisation de l'identité. Techniquement, nous pouvons remplir ce dernier objectif avec un fichier à « lien faible ». C'est pourquoi je remercie les rapporteurs pour leur proposition n° 2.

M. Alain Vasselle. – Aujourd'hui, seules certaines communes établissent les passeports, ce qui entraîne des coûts financiers supplémentaires. A-t-on une idée de la charge ainsi transférée aux communes ? Certains maires estiment qu'il s'agit d'une dépense de centralité et ils demandent aux communes rurales d'y participer.

Les procédures que vous proposez ne vont-elles pas allonger les délais de délivrance des cartes d'identité ?

M. François Bonhomme, rapporteur. – Quelques collectivités ont demandé aux tribunaux administratifs de statuer sur la problématique de délivrance des passeports. Condamné, l'État a dû participer à ce coût. Néanmoins, il n'en supporte qu'une faible partie.

M. Jean-Yves Leconte, rapporteur. – Pour les passeports, il n'y a pas de lien entre le domicile de la personne et la commune dans laquelle la demande est déposée. Les Français de l'étranger déposent ainsi leur demande dans le consulat de leur choix.

Comme l'a dit M. Pillet, le stockage des données est le cœur du problème. Ainsi, les passeports allemands ne sont pas reliés à une base de données.

Nous ne nous rendons pas compte que nous produisons des données biométriques, que ce soit par le téléphone, mais aussi par les équipements électroniques de nos voitures.

M. François Bonhomme, rapporteur. – 3 527 stations de recueil d'empreintes pour les passeports sont déployées sur 2 088 communes et la dotation forfaitaire des titres sécurisés se monte à 5 030 euros par an et par

appareil. Mais, pour fonctionner, chaque poste nécessite la mise à disposition d'agents d'accueil. Nous sommes donc loin du compte.

M. Jean-Yves Leconte, rapporteur. – Le projet de carte nationale d'identité biométrique a été enterré en 2012. Nous avons pris du retard. Pendant ce temps, les technologies avancent et il nous faut revenir sur ce dossier central, sinon nous risquons de ne plus être capables de créer des identités numériques.

M. Alain Vasselle. – *Quid* des délais de délivrance ?

M. Jean-Yves Leconte, rapporteur. – Avec les empreintes enregistrées dans la base, nous pouvons éviter de faire revenir les personnes lorsqu'elles déposent une nouvelle demande de délivrance d'un document d'identité. On règlerait ainsi les problèmes de délais.

M. François Bonhomme, rapporteur. – Les déclarations d'impôt pourraient également comporter l'identité numérique afin de sécuriser le dispositif. Les actes de la vie courante peuvent donc aussi être concernés par notre rapport.

M. Patrick Masclet. – L'État a fixé les 5 030 euros en fonction du temps de connexion des ordinateurs, mais il a oublié de prendre en compte le temps d'accueil et de montage des dossiers. Dans le Nord, si la carte d'identité nationale devenait biométrique, la quasi-totalité des maires rendraient les stations à l'État pour protester contre la faible indemnisation.

M. Philippe Bas, président. – Cette remarque est fort judicieuse.

La commission autorise la publication du rapport d'information.

LISTE DES PERSONNES ENTENDUES ET DU DÉPLACEMENT

Ministère de l'intérieur

M. Éric Tison, sous-directeur des libertés publiques à la direction des libertés publiques et des affaires juridiques (DLPAJ)

Secrétariat général pour la modernisation de l'action publique (SGMAP)

M. Xavier Albouy, chargé de mission auprès de la Direction interministérielle du numérique et des systèmes d'information (DINSI)

Direction des Français de l'étranger et de l'administration consulaire

M. Nicolas Warnery, directeur

M. Sylvain Riquier, sous-directeur de l'administration des Français

Mme Sandrine Lelong-Motta, chargée de mission à la mission pour la politique des visas

Commission nationale de l'informatique et des libertés (CNIL)

M. Émile Gabrié, chef du service du secteur régalien et des collectivités locales

M. Stéphane Grégoire, chef du service du secteur économique

Mme Tiphaine Inglebert, conseillère pour les questions institutionnelles et parlementaires

Agence Nationale des Titres Sécurisés (ANTS)

M. Cyril Murie, responsable du pôle international et innovation

M. Pierre Orszag, adjoint du responsable du pôle titres régaliens

European Foundation for Information Society

M. Manuel Becerril Gonzalez de la Mata, secrétaire général

Alliance pour la Confiance Numérique (ACN)

M. Olivier Clemot, société Safran identity and security

M. Thomas Chenevier, société Safran identity and security

Mme Carole Pellegrino, société Safran identity and security

M. Ugo Dallemagne, société Natural Security Alliance

Personnalités qualifiées

M. Guillaume Desgens, maître de conférences associé au Conservatoire national des arts et métiers (CNAM)

Mme Bernadette Dorizzi, directrice de la recherche et des formations doctorales à l'école Telecom SudParis

Mme Sylvia Preuss-Laussinotte, maître de conférences en droit public à l'université Paris X Nanterre, directrice du master droit des nouvelles technologies et société de l'information

Déplacement à la Gare du Nord *(jeudi 24 mars 2016)*

Ministère de l'intérieur

M. David Skuli, directeur central de la police aux frontières

Mme Isabelle Busson, adjointe du chef de service national de la police ferroviaire, cheffe de la brigade des chemins de fers

M. Stéphane Pidoux, adjoint à la cheffe de la brigade des chemins de fer

M. Stéphane Meguirditchian, adjoint au chef de l'unité des contrôles techniques

M. Pierre-Alexandre Gelas, bureau des projets technologiques

M. Éric Clément, bureau des projets technologiques

Eurostar

M. Mikaël Lemarchand, directeur des gares

M. Carol Jonard, directeur des affaires publiques