NOTE DE SYNTHÈSE

SÉNAT

RÉPUBLIQUE FRANÇAISE

BIOMÉTRIE : METTRE LA TECHNOLOGIE AU SERVICE DES CITOYENS

COMMISSION DES LOIS

Rapport d'information de
MM. François Bonhomme et Jean-Yves Leconte

■ Les **données biométriques** « *ne sont* ***pas des données à caractère personnel comme les autres*** » comme le souligne la Commission nationale de l'informatique et des libertés (CNIL). Elles touchent, en effet, à la sphère de l'intime en permettant la reconnaissance des individus à partir de leurs caractéristiques physiques, biologiques ou comportementales.

■ Le développement des techniques biométriques nécessite ainsi la mise en œuvre d'un **cadre juridique spécifique** pour utiliser toutes leurs potentialités tout en préservant le droit à la vie privée des citoyens.

■ La mission d'information, confiée aux sénateurs François Bonhomme (Les Républicains – Tarn-et-Garonne) et Jean-Yves Leconte (Socialiste républicain – Français établis hors de France), s'est attachée à dresser **un bilan des usages publics de la biométrie** pour analyser la façon dont l'administration utilise ces techniques à des fins judiciaires et administratives (résolution d'enquêtes criminelles, police administrative, simplification des relations entre les citoyens et leur administration, *etc.*).

■ Les rapporteurs concluent que **les potentialités des dispositifs biométriques pourraient être davantage exploitées par l'administration sous réserve de la nécessaire protection de la vie privée**.

Les usages publics de la biométrie se sont progressivement développés

■ La diversification des techniques

Le marché mondial de la biométrie représenterait près de **9 milliards d'euros,** partagés à parité entre les usages publics et les usages privés.

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

De nouvelles techniques de reconnaissance anatomique apparaissent aujourd'hui 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** connaissant l'expansion la plus rapide.

■ Un premier usage dans le domaine judiciaire

La biométrie est d'abord utilisée dans les **procédures criminelles** pour faciliter l'identification des auteurs d'infractions et l'instruction des affaires.

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).

En 2014, le **FAED**, qui comporte les empreintes digitales de **5 millions de personnes**, a par exemple permis d'identifier des individus lors de 14 698 affaires.

JUILLET 2016

■ L'essor des usages administratifs

Depuis le milieu des années 2000, un usage administratif des techniques biométriques s'est ajouté à cet usage judiciaire, notamment sous l'impulsion des États-Unis et de l'Organisation de l'aviation civile internationale (OACI).

La biométrie sert ainsi à **authentifier** et à **identifier les ressortissants français**. **22,6 millions de passeports biométriques** ont été produits entre juin 2009 et avril 2016 et près de 315 000 sont délivrés chaque mois.

Ces techniques sont également utilisées pour **authentifier et identifier les ressortissants étrangers** :

- des **visas biométriques** sont délivrés aux personnes voyageant en France, à partir d'un dispositif expérimenté à compter de 2007 et généralisé en 2015 ;

- le **système EURODAC** permet de déterminer le pays de l'Union européenne compétent pour traiter une demande d'asile.

■ 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.

La **lutte contre les fraudes à l'identité** constitue, en effet, un objectif de politique publique.

Ces fraudes sont d'autant plus préoccupantes qu'elles peuvent servir de support à d'autres infractions comme l'usurpation d'identité, l'escroquerie bancaire, *etc*. En 2014, la direction générale de la police aux frontières (DCPAF) a ainsi intercepté **15 018 faux documents d'identité**.

Les techniques biométriques s'inscrivent également dans la « ***transformation numérique*** » **des services publics**, appelée de ses vœux par la Cour des comptes en 2016 dans une logique de simplification des relations entre les citoyens et l'administration.

La biométrie rend par exemple possible l'automatisation des contrôles aux frontières pour concilier des vérifications approfondies et la forte croissance de la mobilité transfrontalière. À titre d'exemple, les sas automatiques **PARAFE** permettent de **passer une frontière aéroportuaire en toute sécurité en seulement 20 secondes**.

■ Des risques d'erreurs et de fraudes

Pour autant, les données biométriques ne sont pas infaillibles.

Chaque système doit **trouver un équilibre entre des fausses acceptations** (le dispositif n'arrive pas à reconnaître un imposteur et à le rejeter) **et des faux rejets** (il ne parvient pas à identifier une personne éligible et la rejette à tort).

En outre, des **tentatives de fraudes** ne sont pas à exclure. Il est ainsi possible de « *tromper* » le dispositif biométrique, notamment en fabriquant un doigt artificiel imitant l'empreinte digitale d'un tiers (technique du « *faux doigt* »).

Un cadre juridique spécifique

La **donnée biométrique est sensible** car « *à la différence d'une autre donnée d'identité (…), elle 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* » (CNIL).

Les usages publics de la biométrie sont possibles uniquement s'ils sont autorisés par un décret en Conseil d'État pris après avis motivé et publié de la CNIL.

Le Conseil constitutionnel veille, en outre, à ce que les traitements biométriques comportent 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 **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 suffisant (faciliter la recherche des auteurs de certaines infractions).

Tel n'était pas le cas du « *fichier central commun* » regroupant les informations biométriques des détenteurs d'un passeport ou d'une carte d'identité biométriques que la loi n° 2012-410 du 27 mars 2012 visait à créer.

Pour un tel fichier administratif, il est indispensable de privilégier la technique du « ***lien faible*** » qui, à la différence du « *lien fort* », ne permet pas d'identifier une personne à partir de sa seule donnée biométrique.

Mieux exploiter les potentialités des dispositifs biométriques

■ Créer une véritable identité numérique à partir d'une carte d'identité biométrique

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 du 27 mars 2012 relative à la protection de l'identité et dont la création a été validée par le Conseil constitutionnel.

L'exécutif privilégie des mesures alternatives comme le **projet ALICEM** qui permet aux citoyens d'utiliser leur passeport biométrique pour certifier leur identité à partir de leur téléphone portable et accéder à des services administratifs en ligne.

Toutefois, **ces différentes initiatives du Gouvernement ne peuvent se substituer à la création d'une carte d'identité biométrique**, instrument le plus efficace pour lutter contre les fraudes à l'identité. Le coût d'un tel dispositif – environ **85 millions d'euros** – ne paraît pas dirimant au regard des enjeux en cause.

Dans la même logique, le rapport préconise de recueillir les données biométriques des nouveaux titulaires du **certificat de nationalité française (CNF)** afin de sécuriser la « *chaîne de l'identité* ».

■ 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 physique*** » du citoyen en mairie ou dans les consulats pour le recueil de ses empreintes, puis le retrait de son document d'identité. Cette exigence représente une difficulté parfois coûteuse pour les Français établis hors de France et dont la résidence est géographiquement éloignée de leur ambassade et de leur consulat.

Il est donc essentiel de prévoir un **maillage cohérent et efficace des centres de recueil de données biométrique**s. Concernant les visas, l'État a externalisé ses centres de collecte dans les pays de taille importante et les a même mutualisés avec d'autres pays de l'espace Schengen.

Pour être pleinement efficace, cette initiative relative aux visas devrait être étendue aux passeports biométriques.

De même, il est techniquement possible d'éviter un nouveau recueil d'empreintes lors du renouvellement d'un passeport, les données correspondantes étant déjà enregistrées dans un fichier. Dès lors, pourquoi continuer à demander aux citoyens de redonner leurs empreintes à chaque renouvellement ?

■ Développer l'usage de la biométrie à la frontière

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 rapport déplore toutefois **le faible niveau d'interopérabilité des dispositifs biométriques utilisés à l'échelle européenne**.

À titre d'exemple, les autorités françaises ne sont pas en mesure de « *lire* » l'empreinte digitale enregistrée dans un passeport d'un autre État de l'espace Schengen, faute d'échange de certificats de sécurité entre les pays.

Dans ce contexte, le projet européen « ***frontières intelligentes*** » – dont la mise en œuvre concrète est prévue en 2020 – constitue une opportunité à saisir. Il comprend :

- d'une part, **le programme d'enregistrement des voyageurs (RTP)** pour

fluidifier le trafic des personnes dans la logique du dispositif PARAFE ;

- d'autre part, **le système entrée/sortie (EES)** pour enregistrer les passages à la frontière extérieure de l'espace Schengen des ressortissants de pays tiers. Permettant une gestion plus rationnelle des frontières, l'ESS comportera notamment une « *calculatrice automatique* » déterminant automatiquement le nombre de jours passés dans l'espace Schengen et alertant les États dans l'hypothèse où la personne concernée aurait dépassé la période de séjour autorisée.

Reprenant une préconisation de la commission des affaires européennes du Sénat dans son rapport d'information n° 499 (2015-2016), « *L'Europe de Schengen face à la crise des réfugiés* », MM. Bonhomme et Leconte proposent d'**élargir l'ESS aux citoyens européens ainsi qu'aux personnes vivant dans la zone Schengen**.

Sans prévoir un historique systématique de leurs déplacements, 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 de participer à des activités terroristes.

■ Expérimenter la connexion entre vidéoprotection et bases de données

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, toutefois, d'un **instrument pertinent pour prévenir et lutter contre le terrorisme.** Concrètement, il permettrait d'identifier une personne en temps réel à partir d'un dispositif de reconnaissance faciale relié à un fichier contenant les photographies d'individus recherchés.

Conscient des limites techniques de ce dispositif, le rapport propose son **expérimentation dans un cadre juridique strictement défini** : respect du droit applicable à l'installation de caméras sur la voie publique et des règles relatives à la protection des données personnelles, durée d'expérimentation limitée à un an, contrôle de la CNIL, *etc.*

D'un point de vue opérationnel, la **création d'un nouveau fichier** de personnes recherchées serait nécessaire, les traitements de données existants ayant des finalités trop larges ou s'inscrivant dans des procédures judiciaires spécifiques.

Commission des lois
http://www.senat.fr/commission/loi/index.html
Téléphone : 01 42 34 23 37 – Télécopie : 01 42 34 31 47

Rapporteur
François Bonhomme
Sénateur (Les Républicains) du Tarn-et-Garonne

Rapporteur
Jean-Yves Leconte
Sénateur (Socialiste et républicain) représentant les Français établis hors de France

Le présent document et le rapport complet sont disponibles sur internet :
http://www.senat.fr/notice-rapport/2015/r15-788-notice.html