Biométrie et choix de société

Nicola Spanti

Janvier 2017

1 Le fichier TES

1.1 C'est quoi, pour faire quoi, et comment ?

Le fichier TES a pour objet la "création d'un traitement de données à caractère personnel commun aux passeports et aux cartes nationales d'identité", TES étant l'abréviation de "titres électroniques sécurisés". Il est la conséquence du décret numéro 2016-1460 du 28 octobre 2016, décidé sans l'approbation des députés et sénateurs et sans publication en amont d'une véritable étude d'impact (via l'article 27 de la loi du 6 janvier 1978).

Ce fichier regroupera des données issues des procédures pour obtenir une carte d'identité française ou un passport français. Dans son avis, la CNIL fait remarquer que c'est "une base réunissant des données biométriques relatives à 60 millions de personnes, représentant ainsi la quasi-totalité de la population française". Parmi les données du fichier, il y a des données biométriques (article 2 du décret) : la couleur des yeux, la taille, l'image numérisée du visage, et celles des empreintes digitales. L'article 9 précise la durée de conservation : (pour les données à caractère personnel) "15 ans s'il s'agit d'un passeport et 20 ans s'il s'agit d'une carte nationale d'identité", et respectivement 10 et 15 pour les mineurs.

Les raisons de la création de ce fichier sont "l'établissement, à la délivrance, au renouvellement et à l'invalidation des cartes nationales d'identité [...] et des passeports [...], ainsi que prévenir et détecter leur falsification et contrefaçon" (article premier). Mais ce ne sont pas les seuls, il servira aussi aux "missions de prévention et de répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme".

L'authentification, c'est-à-dire vérifier une correspondance, est permise, Néanmoins l'identification, c'est-à-dire chercher une correspondance sans ciblage fin, est illégale (partie 2 de l'article 2).

C'est un fichier administratif, qui pourra donc être utilisé par l'exécutif et la justice. Son utilisation ne se limite pas à la France, il peut être utilisé via INTERPOL et le système d'information Schengen (article 4), mais ce n'est pas le cas des données biométriques (article 4 et 6).

1.2 Critiques

Il s'agit d'un unique fichier au sens propre, une base centralisée. Ainsi, les personnes y ayant accès peuvent potentiellement faire des opérations sur une importante quantité de données personnelles. L'accès légal a des conditions, mais elle pourrait évoluer à l'avenir dans un sens plus ouvert, et il faut aussi prendre en compte l'intensité des potentielles sanctions en cas d'usage illégal avéré. De plus, un tel fichier a une grande valeur, il serait donc particulièrement intéressant à copier et/ou utiliser illégalement pour certaines activités.

La centralisation aurait pu être évitée en stockant les données (chiffrées et signées) uniquement sur des cartes à puces détenus par les individus qu'elles concernent. Cela aurait été moins pratique et plus cher financièrement. Cependant, les données auraient été disséminées et non connectées à un ou plusieurs réseaux sans le moindre doute. De plus, la dissémination aurait été prohibitive pour un élargissement de l'usage des données dans un cadre massif. Il faut ajouter qu'il aurait été assuré que seul l'authentification soit possible et uniquement avec l'accord de la personne concernée, tout en permettant au porteur ou à la porteuse de

détruire ces informations personnelles s'ille le juge nécessaire. C'est par exemple ce qui a été mis oeuvre pour le système Parafe de contrôle aux frontières automatisé.

L'identification avec un système d'authentification centralisé est toujours techniquement possible. En effet, essayer d'authentifier avec A, puis B, et ainsi de suite avec tous les autres, revient à identifer. Par exemple, une authentification réussie avec B revient à l'identifier avec succès, tandis qu'aucune authentification réussie avec tous est un échec d'identification. L'utilisation d'un condensat (aussi appelé hash ou bio-hash dans le cas de la biométrie) ne fait que ralentir (très peu) l'identification, il n'empêche nullement. Néanmoins, une fonction de condensation faible, c'est-à-dire qui produit souvent le même condensat avec des données différentes, peut permettre qu'une tentative d'identification donne plusieurs identités différentes, il faut pour cela bien la choisir, et être conscient qu'un recoupement avec d'autres données peut permettre d'éliminer les fausses identités trouvées (comme l'a plus longuement expliqué François Pellegrini, un membre de la CNIL).

Un système similaire avait été proposé en 2012. Il a été jugé non constitutionnel, notamment car il aurait permis légalement "l'identification d'une personne à partir de ses empreintes digitales", ce qui "porte une atteinte inconstitutionnelle au droit au respect de la vie privée". Certes le decret du fichier TES ne permet légalement que l'authentification, mais techniquement aussi l'identification (pendant une tentative d'authentication où une donné non hashée peut être récupérée), est ce suffisant pour respecter la constitution ?

Il faut également prendre en compte la manière dont est rédigé le decret pour les empreintes digitales. C'est l'image numérisée qui pourra être enregistrée ! Pourtant, il n'est nullement nécessaire d'autant d'information pour un système biométrique digital. Il est par exemple courant de n'enregistrer que les minuties, qui sont des données calcullées lors de l'enrollement dans le système, rendant inutile de garder l'image numérique pour utiliser le système. Il faut néanmoins être conscient qu'il est possible de reconstituer une empreinte digitale à partir des minuties dans une certaine mesure.

Pour rassurer, il a été ajouté la possibilité d'*opt-out* pour les empreintes digitales. Mais celle-ci ne concerne que les cartes d'identité (donc pas les passports). De plus, il est probable qu'il faille fermement le vouloir pour en profiter, en effet la majorité des gens ne s'y opposeront pas (volontairement ou par méconnaissance) et il faut affronter l'impression de pression sociale (notamment de l'agent qui récupère les informations pour le titre), ce à quoi il faudra peut être ajouté des papiers en plus, on peut donc présumer que presque personne n'usera de ce droit. De plus, les personnes sans empreintes dans le fichier pourraient être considérées comme de potentiels suspects.

AMESys va contribuer à faire ce fichier TES, cela pourrait paraitre anecdotique. Cependant, cette société a vendu un système pour surveiller toute une population à la Lybie (qui à l'époque était sous le contrôle de Mouammar Kadhafi). Cela lui vaut d'être attaqué en justice pour "complicité d'actes de torture". Qu'une partie de TES soit donnée à une entreprise aussi peu respectable ne rassure bien évidement pas.

L'ANSSI et la DINSIC affirme que "TES peut être techniquement détourné à des fins d'identifcation, malgré le lien unidirectionnel du lien informatique" (voir page 4 de leur rapport commun du 13 janvier 2017). Ils en profitent pour rappeler qu'il est "impossible de garantir l'inviolabilité technique absolue d'un système d'information dans le temps". Ce système a pour but d'être persistant, il faut donc se baser sur l'espoir qu'à l'avenir personne ne veule en étendre les possibilités. Cela pourrait être possible via des avancés scientifiques, la monté de la puissance de traitement, ou la non mise en oeuvre de sécurité suffisante pour empêcher techniquement l'extension des usages avec l'état de l'art actuel (puisque par volonté politique des fonctions pourront être ajoutées et que l'organisation pourra voler en éclats). Pourtant le risque politique peut sembler grand au vue de certains événements récents (monté du Front National, élection de Trump, État d'urgence qui affaiblit la séparation des pouvoirs au profit de l'exécutif, le comité contre la torture de l'ONU qui est préocupé vis-à-vis de la France, etc.). Un des moyens les plus surs de le faire augmenter est que les dominants ne considère pas utile de faire un débat avec un peuple qui s'en rend compte, en effet il risque d'être énervé d'une telle soustraction à la délibération démocratique et de l'arrogance nécessaire à tel coup d'épée dans le dos, alors que la démocratie lui est chanté à longueur de discours. Puisque même la presse grand public s'est saisie du sujet, le fichier TES a été une fausse note percue.

2 Prise de hauteur

2.1 Biométrie et fichage de masse

Bien qu'évident, il peut ne pas être inutile que les données biométriques de notre corps sont non révocables. Celles-ci sont de plus en plus utilisées, y compris dans des systèmes non gouvernementaux. Cela acroit le risque d'une fuite. L'évaluation de la sécurité d'un système ou d'une information s'évalue souvent via son maillon le plus faible, dans notre cas la base de données biométriques qui sécurise le moins bien. Pour protéger une donnée, il est donc préfèrable qu'elle soit à le moins d'endroit possible, voire nulle part (il n'y a pas à protéger ce qui n'existe pas). De plus, une fuite de données biométriques non unidirectionnelles engendrait la possibilité technique d'identification via d'autres systèmes biométriques. Or il est extrèmement rare (en 2017) de pouvoir vérifier un système biométrique ou faire vérifier par une personne indépendante (physique ou morale), la faute au recours à du logiciel privateur et à l'usage d'ordinateurs sous le contrôle de tiers. La vie privée n'étant pas quelque chose de très important pour une grande partie de la population (pour le constater, on peut comparer le Watergate avec les révélations de Snowden, le premier a engendré une démission et aucune pour le second malgré l'ampleur bien plus grande), donc il n'est pas étonnant qu'un système biométrique tiers n'est pas besoin de certification, il n'en existe de toute façon même pas.

Un fichier regroupant des données personnelles de presque toute une nation implique que le gouvernement (qui le met en place) applique la présomption de culpabilité. L'article 9 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 est "Tout homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi". Or le préambule de la constition de la France renvoie à cette DDHC.

Le fichier TES n'est pas le premier qui soit massif, c'est d'ailleurs la fusion de 2 fichiers. Il y a la biométrie "classique", mais aussi la biométrie dite "douce". Cette dernière s'appuie sur des signes, comme les comportements. En croisant des données, elle permet d'identifier mais d'une manière floue. À défaut de donner des résultats précis, elle peut permettre au moins de catégoriser des individus.

Collecter, croiser et utiliser massivement des données personnelles est devenu courant. Dans les pays capitalistiquement développés, rares sont celles et ceux qui ignorent que les GAFAM (Google, Amazon, Facebook, Apple, Microsoft) sont des aspirateurs à données et que la NSA a mis le monde sur écoute. Ce qui est moins connu, c'est que la France est proche (mais a moins de moyens techniques) : Hadopi, accord Lustre, l'article 20 de LPM de 2013, AMESys, loi sur le renseignement, etc. Comme la NSA avec PRISM et d'autres programmes, la France use aussi des moyens des entreprises qui n'ont parfois même pas peurs de le dire publiquement.

Au 1 place de Fontenoy à Paris (à côté de la CNIL), on peut lire "Dans ce batiment, qui abritait le Commissariat General au Travail Obligatoire, le 25 fevrier 1944, un commando des groupes Francs du mouvement de libération nationale conduit par Leo Hamon détruisit le fichier des jeunes français de la classe 42, susceptibles d'être appelés pour le service du travail obligatoire." Il pourrait être utile de se rappeler quelles ont été les motivations de la destruction de tels fichiers.

Qui est paranoïaque ? Les individus tenant à leur vie privée ? Les États qui avec le fichage de masse considèrent implicitement la population comme un ennemi ?

2.2 Au-delà du numérique

Des organisations (comme la Ligue des Droits de l'Homme et La Quadrature Du Net) alertent sur une regression des droits humains qu'elles jugent de plus en plus préocupantes. En effet, de plus en plus de pouvoir est donné à l'exécutif au détriment de la justice, et un premier ministre a récemment invité à ne pas "risquer" de faire respecter la constition ! L'État a besoin de pouvoir et est utile par bien des manières à la population. Cependant un État dangereux n'a pas besoin de se cacher comme les groupes bien moins gros qu'il considère comme "terroristes", et peut faire bien plus de dommages que ces derniers. Il faut donc veiller à ne pas trop lui donner de pouvoir et au délicat équilibre entre ces 3 composantes dans un État de droit (exécutif, législatif,

et judiciaire), ce qui est un enjeu majeur.

On s'est ici proposé de donner des éléments de débat, mais cette pratique n'est pas bien vue par tous et toutes. "Il ne peut y avoir aucune explication qui vaille. Car expliquer, c'est déjà vouloir un peu excuser." L'implication de cette proposition est qu'il faut arrêter d'expliquer, de réfléchir, il y aura toujours le risque d'excuser. Encore un pas, et il sera dit "l'ignorance, c'est la force". Mais George Orwell n'a pas écrit 1984 comme un manuel à suivre...

Si comme Frédéric Lordon, on postule que "les individus se comportent toujours comme les contraintes dans lesquelles ils sont plongés les conduisent à se comporter et pas autrement", il faut s'attaquer au cadre (qui faconnent les individus) si on veut une autre société (vis-à-vis de la protection des données biométriques, de celles permettant la biométrie "douce" au sens large, et aussi potentiellement d'autres choses). Mais encore faut-il savoir ce que l'on veut, donc réfléchir, philosopher, ce qui n'est pas considéré important dans le cadre actuel. Les questions techniques et leurs réponses ne donnent pas d'elles-mêmes un sens à la vie, or après l'école et dans les formations en sciences "dures" (comme l'informatique), il n'est question que d'elles ou presque, malgré le fait qu'elles ne sont nullement nécessairement porteuses d'un monde meilleur. L'éducation populaire, ils n'en ont pas voulu, mais peut être faudrait il y venir.

3 Sources

Une grande partie de mes sources est citée au fur et à mesure sous forme de texte ou de lien hypertexte. Elles sont plus ou moins directement issues de ma veille sur le fichier TES (NextINpact, l'ANSSI et la DINSIC, la CNIL, Les exégètes amateurs, le site web reflets.info, etc.).

4 Licence