REE REVUE DE L'ÉLECTRICITÉ ET DE L'ÉLECTRONIQUE

Accès contrôlé par reconnaissance d'identité à partir des caractéristiques de l'iris – Source Cern Document Server.

Un nouvel espace d'identification de masse

Introduction

Marc Leconte
Membre émérite de la SEE

Les technologies biométriques qui se diversifient sans cesse envahissent peu à peu notre vie quotidienne. Cela pose des problèmes à la fois des problèmes techniques en termes de fiabilité d'identification mais aussi éthiques du fait des menaces que ces technologies peuvent faire peser sur les libertés publiques de l'individu si elles sont mal contrôlées.

Commençons par une définition : La technologie biométrique consiste à transformer une caractéristique biologique, morphologique ou comportementale en une empreinte numérique. Mais Le terme « biométrie » est de plus en plus utilisé pour définir des techniques permettant d'identifier une personne à partir de l'un ou plusieurs de ses caractères biologiques ou comportementaux alors même que la biométrie recouvre un champ scientifique beaucoup plus vaste. Le terme « biométrie » a été introduit dans le vocabulaire scientifique à la fin du dix-neuvième siècle et correspond aux mots anglais « *biometry* » ou « *biometrics* » employés parfois par les auteurs américains comme des synonymes du mot « statistiques ». Dans la langue française, plusieurs acceptions sont données : « étude mathématique, surtout statistique, des phénomènes biologiques » (dictionnaire Hachette), « science qui étudie à l'aide des mathématiques (statistiques et proba-

bilités) les variations biologiques à l'intérieur d'un groupe déterminé » (dictionnaire Robert).

L'extension de la biométrie

Si l'identification et le fichage par empreinte digitale sont très anciens, aujourd'hui la biométrie se fonde sur la mensuration et le dénombrement et elle utilise les statistiques et les probabilités. Les données biométriques susceptibles de servir à une identification se diversifient. Alors qu'il y a encore 50 ans la topographie du système pileux, la couleur des cheveux, la pigmentation des yeux ne constituaient pas des caractères mesurables, aujourd'hui, aucun caractère ne semble *a priori* exclu.

Les données biométriques ne sont plus nécessairement anatomiques, la voix, le geste, l'odeur, la chaleur sont désormais aussi pris en compte et les photographies numérisées sont maintenant utilisées pour la reconnaissance faciale. Un autre apport des technologies informatiques est l'automatisation et son corollaire la massification du traitement des données. L'automatisation permet par ailleurs d'effectuer des traitements de masse rapidement, voire presque instantanément, dans des domaines où le patient et minutieux travail d'expertise semblait réservé à l'expert. Si les technologies biométriques sont définies comme des systèmes de reconnaissance automatique, le degré d'automaticité est lui-même devenu un critère de qualification.

Depuis la généralisation de ce qu'on appelle les techniques numériques, on assiste à l'élargissement des domaines d'application des systèmes biométriques d'identification. En effet l'utilisation des procédés d'identification humaine a été longtemps cantonnée aux applications militaires et policières. L'identification humaine, celle des récidivistes d'abord, celle des malfaiteurs ensuite, grâce aux traces abandonnées par eux sur les lieux d'infraction, a été dès l'origine la préoccupation majeure des services de police technique ou scientifique. Dans ce domaine d'ailleurs, les besoins d'identification ne se limitent plus à la seule répression des atteintes à la sécurité publique, mais s'étendent à leur prévention. Mais l'utilisation des réseaux, en particulier internet, à l'échelle de la population mondiale, a élargi le domaine de la biométrie. Ainsi pour répondre aux besoins d'identification et d'authentification dans le monde numérique, divers moyens ont été mis en œuvre (codes, mots de passe, numéros d'identification, cartes, signature numérique…) et les systèmes biométriques sont susceptibles de les remplacer ou de les sécuriser.

Ces besoins d'identification s'inscrivent dans un cadre spatial plus ou moins large, ils peuvent être circonscrits à un bâtiment ou un réseau restreint comme prendre une dimension internationale par l'effet de l'intensification de la circulation transfrontalière des hommes et la mondialisation des échanges de biens et de services. Ils doivent, par ailleurs, se concilier avec d'autres besoins, tels que le respect de la vie privée, la protection des données personnelles, les libertés individuelles.

Les problèmes éthiques

C'est ce dernier point, l'intrusion de systèmes biométriques dans la sphère de la vie privée, qui est une source à la fois de sécurisation extrême et de craintes multiples. Il y a donc un débat qui est tout d'abord de nature technique. Les systèmes biométriques d'identification sont-ils fiables ? Sont-ils plus performants que les méthodes d'identification habituellement pratiquées ? Parmi les différentes techniques, quelles sont celles qui semblent les plus sûres et les plus pratiques au regard de l'usage que l'on veut en faire ? Une autre question se pose également avec une dimension sociétale plus importante qui est de déterminer si tout ce qui est possible techniquement doit être développé à grande échelle.

Le corollaire de cette question est que ce qui est techniquement possible est, ou sera développé quelque part dans le monde d'où l'idée qu'il faut réguler ces technologies par divers moyens démocratiques de surveillance car ce serait une naïveté de penser que l'éthique bloque de manière générale les avancées technologiques. Les dictatures font également de la science et de la technologie. Face à ces interrogations le grand public sait aujourd'hui que les Etats, fussent-ils démocratiques et, à plus forte raison les autres, ne sont pas arrêtés par ces considérations. En effet Les révélations en juin et juillet 2013 concernant l'accord permettant à la *National Security Agency* (NSA) américaine d'accéder directement aux serveurs de neuf géants de l'Internet (courriers électroniques, chats vidéo et audio, photos, transferts de fichiers) ont mis au jour des logiques qui étaient jusqu'alors restées implicites, à savoir l'élargissement du champ du renseignement en accentuant l'intrusion dans la sphère intime de chacun, en contribuant par là même à légitimer une réduction de la confidentialité de la vie privée au nom de la protection des individus et des organisations.

En France, la loi de programmation militaire institue à sa façon une même possibilité d'intrusion dans nos espaces de vie numérique. Cette loi, promulguée par le président de la République le 18 décembre 2013, permet aux services de l'État (au sein des ministères de la Défense, de l'Intérieur, de l'Économie et des finances) d'accéder aux données informatiques des citoyens sans demander l'avis d'un juge. Nos activités en ligne (nos recherches sur Google, nos courriels, nos achats, etc.) peuvent de la sorte être légalement surveillées. Cette loi n'est pas seulement hautement problématique d'un point de vue éthico-politique, puisqu'elle confirme la détérioration d'un droit à l'opacité, mais elle compromet également un équilibre social basé sur le respect de valeurs qui ont forgé à travers le temps la construction des démocraties modernes.

Parmi celles-ci, *le droit au secret* comme le souci de préserver un minimum de confiance dans les échanges sont essentiels. Les Etats ont donc constitué à partir des nouvelles technologies des fichiers dits de sécurité publique. Il faut rappeler que les fichiers contenant des données à caractère personnel établis par les services publics en charge des questions de sécurité sont une réalité ancienne. Dès le XVIIIème siècle, les autorités instituent divers systèmes d'enregistrement des personnes pour lutter contre ●●●

la criminalité, la mendicité ou l'errance à la fin du XIXe siècle. Ce processus s'amplifie avec le bertillonnage qui rationalise les techniques policières d'identification. Les forces de l'ordre vont alors constituer de vastes fichiers contenant notamment les données corporelles de nombreuses catégories d'individus, délinquants et criminels, vagabonds, individus soupçonnés d'espionnage, anarchistes.

La décision prise, à la fin des années 1960, par le ministère de l'Intérieur d'informatiser nombre de ses ressources documentaires constitue une autre étape décisive en matière d'exploitation des données individuelles à des fins de sécurité. La loi « Informatique et libertés » du 6 janvier 1978 et l'avènement de la Cnil vont apporter un dispositif régulateur que nous évoquions plus haut. Ce sera un tournant majeur en France : une autorité extérieure à la police disposera désormais d'un droit de regard et de contrôle sur les informations qu'elle collecte, archive et utilise. Dans les années 90 on a assisté à un développement considérable des fichiers (personnes recherchées, terrorisme, empreintes génétiques et digitales) auquel viennent s'ajouter récemment les bases de données biométriques. Il est donc indispensable pour le citoyen de connaître et comprendre comment fonctionnent ces nouveaux moyens de reconnaissance basées sur le corps humain afin d'avoir un avis éclairé sur ces dispositifs.

Dans le dossier qui suit nous proposons quatre articles qui traitent certains aspects de la biométrie d'aujourd'hui qui font l'objet de recherches dans les cercles universitaires.

Le dossier biométrie

• Le premier article de **Bernadette Dorizzi** expose les différents systèmes de biométrie et leurs propriétés. La biométrie compare des caractéristiques physiques mesurées et numérisées à une mémoire afin de procéder à une identification. L'auteure passe en revue les principaux caractères physiques utilisés aujourd'hui pour l'identification (visage, empreintes digitales, iris) et souligne les progrès importants réalisés aujourd'hui par les systèmes biométriques car il importe en matière de sécurité de ne pas se tromper afin de pouvoir déjouer des falsificateurs.

• Le deuxième article de **Yaneck Gottesman**, **François Lamare** et **Bernadette Dorizzi** présente un nouveau capteur basé sur une technique de tomographie par cohérence optique (OCT) qui permet une analyse en profondeur donnant accès à l'empreinte digitale profonde qui n'a que peu de risque d'être contrefaite et échappe aux défauts du doigt sale ou abimé. Cette technique en outre détecterait un doigt coupé factice, donc non irrigué. Basé sur un senseur laser, ce détecteur fait appel au traitement du signal classique comparable à celui qui est utilisé, toutes choses égales par ailleurs, pour les lidars.

• Le troisième article de **Joannes Falade**, **Christophe Charrier** et **Christophe Rosenberger** concerne la sécurité et la falsifiabilité des systèmes biométriques. Les auteurs décrivent les différents types d'attaques des systèmes et les manières de s'en prémunir.

• Le quatrième article, par **Christophe Charrier** et **Christophe Rosenberger**, évoque le domaine de la biométrie comportementale qui travaille sur des données caractérisant le comportement de l'individu qui pourraient sembler assez loin d'une caractérisation scientifique. La manière de taper sur un clavier, d'utiliser des objets connectés ou encore la façon de marcher, tout cela fait partie du comportement et il existe des techniques, décrites dans l'article, qui permettent de les identifier et de les rattacher à un individu. Il serait même possible à travers les réseaux numériques d'identifier une personne à distance par la façon de taper sur un clavier. On comprend que de tels systèmes peuvent à juste raison susciter encore plus de réserve du grand public et les auteurs ne manquent pas d'évoquer ce problème dans leur article. ■

L'auteur

Marc Leconte est ancien secrétaire du club RSSR de la SEE (radars, sonars et systèmes radioélectriques), membre du comité de rédaction de la REE, membre émérite SEE et médaillé Ampère. Au sein de Dassault Electronique, il a passé une quinzaine d'années à l'étude, au développement et aux essais en vol du radar RDI du Mirage 2000. Ensuite pendant trois ans, il a participé à l'étude d'un démonstrateur laser franco-britannique CLARA. A partir de 1995, il a élargi son activité aux domaines des études concurrentielles et stratégiques dans les domaines des radars aéroportés et de la guerre électronique. Il a exercé les mêmes activités dans la division aéronautique de Thales après la fusion de Dassault Electronique et de Thomson-CSF. A partir des années 90 et en parallèle, il s'est intéressé à l'histoire des sciences et des techniques et a publié plusieurs articles s'y rapportant.

Les articles