

# La biométrie placée en liberté surveillée ?

Par Paul Lanois

Etudiant du Magistère de Droit des Activités Economiques - Paris I

E-mail : [paulanocom@aol.com](mailto:paulanocom@aol.com)

Lorsque l'on évoque la biométrie, on songe immédiatement aux films de science-fiction. Pourtant, force est de reconnaître que la biométrie fait petit à petit son entrée dans la vie quotidienne, au point que l'on voit maintenant arriver sur le marché des ordinateurs portables avec déverrouillage par empreinte digitale et même des disques durs sécurisés par empreinte digitale.

Par ailleurs, les utilisations de techniques biométriques à grande échelle sont bien réelles, comme l'illustre l'expérimentation actuelle du dispositif de passage rapide de la frontière à l'aéroport de Roissy ou l'utilisation à l'aéroport de Nice Côte d'Azur d'un système de carte de fidélité avec reconnaissance de l'empreinte digitale. On parle même de remplacer la carte d'identité actuelle par une carte à puce intégrant empreintes digitales et photo (carte INES) et de généraliser l'emploi de visas biométriques.

Cependant, le recours à cette technologie n'est pas sans poser de nombreuses questions juridiques. En effet, aucun texte juridique ne vient encadrer la biométrie spécifiquement, ce qui laisse planer de nombreuses incertitudes, notamment au regard des libertés individuelles.

Mais commençons par le début : qu'est-ce que la biométrie ? Concrètement, elle peut être définie comme la technologie qui permet de reconnaître une personne immédiatement à partir de ses caractéristiques uniques, à savoir ses éléments physiologiques ou comportementaux propres tels que ses empreintes digitales, la voix ou l'iris de l'œil. On peut classer les techniques biométriques en trois catégories : celles fondées sur l'analyse de traces biologiques (tels que l'ADN ou la salive), celles fondées sur l'analyse morphologique (reconnaissance de la main, de la rétine, etc.) et enfin celles fondées sur le comportement (reconnaissance vocale, dynamique des frappes au clavier, etc.).

Le principal enjeu de l'utilisation de ces techniques est la vérification et l'authentification des personnes. Les possibilités offertes sont en effet multiples : plus besoin d'avoir recours à des clés ou des codes secrets complexes pour accéder à des données confidentielles ou à des locaux protégés, pas de doute en principe sur l'identité de la personne, pas de pertes de temps inutiles en cas de perte ou d'oubli, et pour couronner le tout, une sécurité accrue puisque les erreurs ou les fraudes devraient être plus difficiles à commettre. Cela permet également de lutter plus efficacement contre la criminalité et le terrorisme.

Pourtant, si les techniques biométriques peuvent apporter une plus grande sécurité, elles peuvent aussi se révéler redoutables pour nos libertés et notre vie privée.

Au niveau européen, la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995<sup>1</sup> considère que le traitement des données à caractère personnel, dont les systèmes biométriques, « sont au service de l'homme; qu'ils doivent [...] respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée ». L'article 6 stipule que « les données à caractère personnel [...] collectées pour des finalités déterminées, explicites et légitimes doivent être [...] adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ultérieurement ». Enfin, conformément à l'article 28 de cette directive, les États membres doivent mettre en place des autorités de contrôle chargées de « surveiller l'application, sur leur territoire, des dispositions adoptées par les États membres en application de la directive. Ces autorités exercent en toute indépendance les missions dont elles sont investies ».

---

<sup>1</sup>Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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 : [Europa.eu.int](http://europa.eu.int), <[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type\\_doc=Directive&andoc=95&nu\\_doc=46](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&andoc=95&nu_doc=46)>.

C'est ainsi qu'en France, la loi « Informatique et Liberté » (n° 2004-804) du 6 août 2004<sup>2</sup> a été modifiée pour que l'utilisation des technologies biométriques soit réglementée par la *Commission Nationale de l'Informatique et des Libertés* (CNIL). La reconnaissance biométrique doit faire l'objet d'une autorisation préalable de la CNIL. La grande innovation est que le nouveau texte a substitué la notion de « *données nominatives* » par celle de « *données à caractère personnel* », c'est-à-dire une « *information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ».

La CNIL a par la suite été amenée à préciser les conditions requises pour obtenir une telle autorisation. Lors de sa séance plénière du 8 avril 2004<sup>3</sup>, elle admet que, « *d'une manière générale, le recours à la biométrie associée aux nouvelles technologies peut être de nature à apporter une réponse adaptée à certaines situations dans lesquelles l'identification des personnes doit être parfaitement assurée* ». Toutefois, elle a indiqué que « *seul un impératif particulier de sécurité est susceptible de justifier la centralisation de données biométriques.*»

Autrement dit, en l'absence d'un impératif de sécurité incontestable, la CNIL se montre prudente envers la création d'une base de données centralisée d'empreintes digitales car celle-ci est susceptible d'être utilisée à des fins étrangères à sa finalité première. Par contre, en présence d'une base de données, la CNIL vérifie si ces techniques sont « *adaptées et proportionnées à la finalité assignée au dispositif* »<sup>4</sup> avant de donner son autorisation.

Par ailleurs, elle se montre favorable aux dispositifs qui stockent les données sur un support individuel ou qui ne laissent pas de traces telles que la reconnaissance du contour de la main ou de l'iris.

Dans sa délibération n°04-018 du 8 avril 2004, elle a refusé la mise en place, par un centre hospitalier, d'un dispositif de reconnaissance de l'empreinte digitale pour la gestion des horaires de son personnel. Elle relève en effet que les données seront enregistrées « *non pas sur un support individuel (tel qu'une carte à puce) détenu par la personne concernée, mais dans le lecteur d'empreintes digitales qui, comme une base de données centralisée, n'est pas de nature à garantir la personne concernée contre toute utilisation détournée de ses données biométriques.* »

De la même façon, la CNIL s'est opposée à la mise en œuvre d'un système de contrôle d'accès à une cantine scolaire reposant sur l'enregistrement dans une base de données des empreintes digitales des élèves. En revanche, elle a autorisé la mise en place d'un dispositif de contrôle d'accès à une autre cantine scolaire par reconnaissance du contour de la main<sup>5</sup> : la géométrie de la main ne laisse pas de traces dans la vie courante contrairement à l'empreinte digitale et ne peut donc être détournée de sa finalité première.

Concernant les aéroports, la CNIL a autorisé, dans sa délibération n°04-017 du 8 avril 2004, la mise en œuvre d'un contrôle d'accès biométrique aux zones réservées de sûreté des aéroports d'Orly et de Roissy reposant sur un système de reconnaissance de l'empreinte digitale, après avoir relevé que « *le gabarit de l'empreinte digitale n'est stocké que sur une carte individuelle (badge) détenue par l'employé concerné* ». C'est ainsi qu'un décret du 27 mai 2005<sup>6</sup> est venu autoriser la création à titre expérimental d'un traitement automatisé de données à caractère personnel relatives à des passagers de l'aéroport de Roissy - Charles-de-Gaulle qui résident dans l'un des Etats de l'Union européenne ou dans la Confédération suisse et qui se sont volontairement inscrits au programme d'expérimentation.

Ce *Programme d'Expérimentation d'une Gestion Automatisée et Sécurisée* (P.E.G.A.S.E.) est destiné à améliorer les conditions du passage de la frontière et la fiabilité des contrôles. Les empreintes digitales (« *minuties des empreintes digitales des index posés à plat* ») des personnes inscrites au

<sup>2</sup> Loi n° 2004-804 du 6 août 2004 (Informatique et Liberté) : *Cnil.fr*, <<http://www.cnil.fr/index.php?id=301>>.

<sup>3</sup> Délibération n°04-017 et n°04-018 du 8 avril 2004 : *Cnil.fr*, <<http://www.cnil.fr/index.php?id=1551>>.

<sup>4</sup> Délibération n°04-018 du 8 avril 2004 : *Cnil.fr*, <<http://www.cnil.fr/index.php?id=1550>>.

<sup>5</sup> Avis du 15 octobre 2002 : *Cnil.fr*, <<http://www.cnil.fr/index.php?id=1422>>.

<sup>6</sup> Décret n° 2005-556 du 27 mai 2005 portant création à titre expérimental d'un traitement automatisé de données à caractère personnel relatives à des passagers de l'aéroport Roissy - Charles-de-Gaulle : <<http://www.admi.net/jo/20050528/INTD0500133D.html>>.

programme ne seront enregistrées et conservées sous forme de fichiers informatiques que pendant la durée de l'expérimentation (un an), soit jusqu'en mai 2006.

Par ailleurs, la CNIL a autorisé, le 7 juin 2005, l'utilisation d'une carte de fidélité stockant l'empreinte digitale du titulaire de ladite carte. Cette carte de fidélité, intitulée "*Club Airport Premier*", permet aux voyageurs de l'aéroport de Nice - Côte d'Azur de cumuler des points pour chaque voyage effectué et de bénéficier de services supplémentaires. Elle a considéré que ce système ne présentait pas de risques particuliers pour la protection des libertés dans la mesure où « *seules les données à caractère personnel des personnes volontaires sont traitées* » et « *l'empreinte digitale est uniquement stockée dans un support individuel exclusivement détenu par la personne concernée (en l'espèce la carte de fidélité) et dont elle décide librement de l'utilisation* ». En effet, il n'y a aucune centralisation des données puisque celles-ci sont stockées sur la carte. Même en cas de vol de la carte de fidélité, il n'est pas possible de recréer l'empreinte digitale et il n'est pas possible non plus d'utiliser la carte sans l'empreinte digitale.

La CNIL n'est pas la seule à contrôler l'usage des techniques de biométrie. Ainsi, par un jugement du 19 avril 2005<sup>7</sup>, le Tribunal de grande instance de Paris a interdit l'utilisation d'un système de pointage utilisant l'empreinte digitale de ses salariés pour contrôler leur temps de présence dans l'entreprise *Effia Services*, filiale de la SNCF. L'entreprise avait mis en place un système de biométrie avant la nouvelle loi Informatique et Liberté du 6 août 2004 et était donc simplement soumise au régime de la déclaration ordinaire.

Les juges ont d'abord énoncé qu'une « *empreinte digitale constitue une donnée biométrique morphologique qui permet d'identifier les traits physiques spécifiques qui sont uniques et permanents pour chaque individu* » et que « *son utilisation porte ainsi atteinte aux libertés individuelles* », même si une finalité sécuritaire ou protectrice de l'activité est exercée dans des locaux. Mais ils ont ensuite estimé qu'en l'espèce, la finalité du système de badge était la gestion des horaires de travail des salariés et que la constitution de la base de données n'était donc « *ni adaptée ni proportionnée au but recherché* ».

Il convient de noter que ce jugement a été rendu sur le fondement de la directive européenne sur la protection des données personnelles ainsi que de l'article L. 120-2 du Code du travail qui énonce que « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*. »

Cette décision, la première sur la biométrie en entreprise, rejoint la position de la CNIL et devrait faire jurisprudence. La biométrie est une technologie sensible, notamment au regard des libertés individuelles, et son usage doit donc être encadré par le principe de proportionnalité.

Pourtant, l'évolution du droit en matière de biométrie est loin d'être toute tracée. En effet, malgré l'existence d'une directive européenne et de la nouvelle loi Informatique et Libertés, le débat est loin d'être clos en l'absence d'un cadre législatif spécifique régissant les différentes applications de la biométrie.

P.L.

---

<sup>7</sup> TGI Paris, 19 avril 2005, Comité d'entreprise d'Effia Services, Fédération des Syndicats SUD Rail c/ Société Effia Services : *Juriscom.net*, <<http://www.juriscom.net/jpt/visu.php?ID=700>>.