L'appréhension par le droit, de la preuve sur les réseaux numériques, Approche technico-juridique[1]

Par Séverine Mas
Avocat au Barreau de Marseille
www.euro-counsels.com

Email : severine.mas@euro-counsels.com

Introduction

Droit et technique sont intimement liés depuis dix ans d'essor des NTIC et le modèle économique développé grâce aux réseaux numériques a entraîné des réformes majeures de pans entiers de notre droit positif. Il en est ainsi du droit de la preuve.

Mais la pensée juridique a évolué de l'enthousiasme initial vers une suspicion par rapport à ces techniques. Le droit français peine à anticiper, englober et surtout comprendre, les phénomènes qui agitent le monde virtuel.

La France d'il y a dix ans était à la pointe en matière de télécommunications (*Alcatel* inventeur de l'ADSL), de cryptographie (l'inventeur de la puce électronique, est le français Roland Moreno), d'informatique. Elle voit ses entreprises rachetées par des groupes étrangers et des technologies de pointe, porteuses d'emploi, s'évader outre-atlantique avec la fuite des cerveaux qu'elle entraîne.

Ceux qui ont peur de ces techniques se sont peut-être trompés d'ennemis : la cryptographie a montré ses limites. Il reste à savoir ce que peut nous apporter la biométrie.

Il est utile de rappeler, en marge de ce colloque, qu'à la *Cité des sciences et de l'industrie* à Paris se tient jusqu'au mois de septembre une exposition sur la biométrie où les techniques utilisées peuvent être expérimentées. Les développements pratiques dans le monde sont également abordés, ainsi que le débat juridique autour de ces techniques.

J'ai pu y constater que la biométrie en l'état actuel utilise des procédés pas toujours très fiables, le nombre de faux rejets étant très important. Je n'ai pu être identifiée par aucune des méthodes : empreintes digitales, contour du visage, ou scannérisation de l'iris.

Mais en fin de compte, il est certain que les implémentations toujours plus nombreuses rendent cette évolution inévitable.

L'avènement de la biométrie dans les technologies - non plus d'identification de l'individu - mais permettant le prolongement même de sa personne dans un double virtuel, fait naître un débat qui pourrait être résumé en deux questions :

1°) Le dédoublement virtuel sécurisé de la personne dans un monde de plus en plus dématérialisé peut il être appréhendé par le cadre législatif actuel ?

2°) Notre société a-t-elle intérêt à permettre cette évolution ?

A la première question, il peut paraître facile de répondre que le cadre est inadapté, mais le travail du juriste ne peut s'arrêter là. Quelle évolution faut-il donc prévoir pour le rendre utile à la fois à la société et à l'individu, en préservant le fragile équilibre entre l'intérêt industriel et l'intérêt général incarné dans le respect des « libertés publiques » ?

1 Ce texte est la transcription de l'intervention qui a eu lieu le 16 juin 2006 dans le cadre du colloque « *Internet sous haute surveillance* », organisé par Me Séverine Mas et le réseau d'avocats *Euro-Counsels* et en partenariat avec l'*Ordre des avocats* au Barreau de Marseille. Pour plus d'authenticité, il n'a été que peu remanié.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>

À la deuxième question, il est clair que nous ne nous sommes même pas **posés** cette question. La biométrie a fait irruption dans nos vies au lendemain des attentats de 2001 et faisant suite aux exigences des américains.

Les pays européens ont d'ailleurs annoncé leur volonté de s'aligner sur la position des Etats-Unis et d'imposer un visa biométrique aux ressortissants étrangers. En France, le ministre des Affaires étrangères, Philippe Douste-Blazy, a ainsi déclaré vouloir « *généraliser le système de visas biométriques à tous les consulats pour 2007* ».

L'intérêt du citoyen de détenir une carte à puce contenant ses identifiants biométriques pour des raisons commerciales, administratives voire ludiques, est un argument bien peu convaincant pour nous autres, juristes et avocats, qui sommes confrontés peut-être plus que d'autres, aux abus et à la délinquance sous des formes multiples. La fraude à l'identité biométrique aurait des conséquences bien plus graves que la fraude à la carte bancaire.

La généralisation de ces procédés pourrait créer plusieurs catégories de citoyens. Ceux qui seraient en dehors du système en seraient totalement exclus.

Mais par ailleurs, l'espionnage à grande échelle de l'Internet, notamment par le *réseau Echelon*, a mis en avant la nécessité vitale de protéger la vie privée des citoyens mais aussi des entreprises.

En 2002, Brian Gladman, ancien "*directeur des communications électroniques stratégiques*" du ministère de la Défense britannique et de l'OTAN, avait publié en ligne un guide pratique de contre-surveillance[2] particulièrement détaillé. Il se justifiait au motif que la cybersurveillance est « *techniquement inepte, inefficace contre les criminels tout en minant la vie privée et la sécurité des honnêtes citoyens et du business* ».

La nécessité d'inscrire dans le droit une preuve numérique sécurisée, peut-être basée sur la biométrie, et de protéger les personnes, physiques ou morales, contre les atteintes à leur vie privée, pose donc concrètement la problématique que notre droit doit résoudre.

Etudions donc d'abord comment la preuve numérique est appréhendée en droit français.

I. La preuve numérique dans le droit français

Comment est incarnée la preuve numérique sur les réseaux ?

La preuve numérique peut englober plusieurs types de documents qui se superposent : - les preuves laissées sur notre disque dur, - celles disséminées au hasard du réseau, - celles envoyées à notre insu aux sites que l'on visite ; - celles envoyées de notre plein gré ; - celles qui sont archivées.

A. La preuve numérique appliquée aux réseaux ouverts

Le véritable débat au sujet de la preuve électronique est de savoir si elle doit être considérée comme plus fiable - *a priori* - que la preuve littérale ou par écrit. Le droit de la preuve numérique est né en France avec la carte bancaire. Le code à quatre chiffres ou code PIN (*personal identification number*) tenant lieu de signature manuscrite. L'utilisation du code secret a été jugée si sûre que ce type de protection a été choisi en France pour le déclenchement de la force de frappe nucléaire, plutôt que la signature manuscrite[3].L'article 4-1 d'une recommandation de la Commission des Communautés européennes du 17 novembre 1988 concernant les systèmes de paiement et notamment, les relations entre émetteurs et titulaires de cartes de crédit, instaure une présomption d'abandon imprudent de son code d'accès par son titulaire, en cas d'utilisation de la carte par un fraudeur à l'aide du code PIN. Cela exonère la banque de toute responsabilité.

L'émergence des réseaux ouverts a engendré la nécessité d'une réforme majeure.

---

2 LSQ : sortez couvert ! ou Comment passer outre la cybersurveillance et les mesures anti-crypto de la LSQ, Bugbrother.com, 17 juillet 2002., <http://www.bugbrother.com/archives/sortezcouvert.html>.

3 Françoise Chamoux, La preuve dans les affaires, de l'écrit au microfilm, Litec Droit 1979.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>

Le Code civil a consacré, aux articles 1316-1 et suivants, les effets de la dématérialisation de la société en insérant plusieurs dispositions en apparence révolutionnaires, destinées à reconnaître l'écrit électronique et la signature du même genre (insérées par Loi nº 2000-230 du 13 mars 2000 art 1 Journal Officiel du 14 mars 2000).

En cas de conflit entre différentes preuves, l'article 1316-2 du Code civil établi par cette loi dispose : « *Lorsque la loi n'a pas fixé d'autres principes et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable quel qu'en soit le support* ».

La charge de la preuve reste donc la question centrale qui vaut tout aussi bien dans le cadre de la cryptographie que de la biométrie. Le législateur de l'an 2000 s'est arrêté en cours de route, en laissant peser la charge de la preuve, dans le cas du commerce en ligne, sur celui qui n'est pas le maître du système d'information.

L'irruption de la biométrie dans les technologies d'authentification aggrave cette faiblesse législative.

Il y a donc aujourd'hui un grand nombre de types différents de preuves numériques de niveau égal et une preuve qui bénéficie d'une présomption de fiabilité établie par le texte de 2000, mais qui est très peu utilisée sur réseaux ouverts, encore moins dans le cadre du *B to C* (boutique vers consommateur).

B. Typologie des modes de preuve numérique

Les preuves et traces laissées sur les réseaux numériques n'obéissent à aucune hiérarchie et sont même parfois générées à l'insu de l'internaute.

1. Les preuves générées à notre insu

a. Les cookies

Les *cookies* sont un élément indispensable à la navigation : il est parfois impossible d'accéder à des sites Internet si l'option « *accepter les cookies* » de votre navigateur est désactivée. Ils sont si inévitables que finalement, ils ont fini par nous apparaître comme des utilitaires innocents; par ailleurs leur nom tend à vouloir nous le faire croire, « *cookies* » signifiant biscuit en anglais. Ceci est une erreur.

Très récemment, il a été mis à jour que les sites gouvernementaux américains, tels que la CIA, la NSA et différents ministères, avaient pisté les internautes connectés à leurs sites Internet, en utilisant des *cookies* permanents. Les *cookies* sont des fichiers texte envoyés sur le disque dur de l'internaute par le serveur auquel il se connecte (qui héberge le site Internet visité), et permettent par exemple, de l'identifier lors d'une nouvelle visite.

Ces *cookies* sont considérés comme des fichiers-espions, leur objet est bel et bien de collecter des informations sur le comportement en ligne.

Les *cookies* envoyés par les sites gouvernementaux américains étaient permanents : ceci leur était pourtant strictement interdit dans le cadre d'une loi de 2003 (*OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, <http://www.whitehouse.gov/omb/memoranda/text/m03-22.html>) - par ailleurs accessible en ligne pour les courageux que cela intéresse et qui prendront ainsi le risque d'être pistés par le gouvernement américain.

Ces *cookies* avaient été paramétrés par une société commerciale de surveillance du web, dénommée « *WebTrends* » ; Parmi les clients de celle-ci, figure le groupe *Hilton*. Une enquête a été ouverte afin de savoir si les *cookies* ont pu mettre en corrélation les visites des internautes sur d'autres sites Internet, notamment commerciaux. Il est évident que le croisement de ces informations permettraient de faire des études comportementales très poussées sur telle personne, identifiée par son *cookie*.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>

Le *cookie* peut enregistrer l'adresse IP (*Internet Protocol*) de l'ordinateur – qui, si elle est fixe, c'est le cas dans une connexion câble ou ADSL - donne l'origine géographique de la personne ; le système d'exploitation ; le nom donné à la machine voire, son utilisateur connecté par exemple dans le système d'exploitation Win XP ; l'heure de la connexion et sa durée ; les pages visitées ; les mots de passe et les login utilisés sur le site ... et ce, à chaque nouvelle visite.

Il ne s'agit pas ici de déterminer le cadre juridique du *cookie* en tant que moyen de collecter une information nominative ou pas. Il est évident que le *cookie*, utilisé dans le commerce électronique, collecte des informations nominatives, dès lors que vous êtes enregistré comme utilisateur habituel ou que vous donnez votre numéro de carte bleue à la fin d'une transaction.

Il faut rappeler en effet, que l'information nominative suivant l'article 4 de la Loi « Informatique et Libertés », est celle qui permet « *sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques* ».

Le *cookie* est un moyen de collecter une information nominative et le consommateur ne peut y échapper : sans *cookie*, pas de navigation possible sur la plupart des sites Internet.

Il est surprenant que la CNIL n'ait jamais considéré le *cookie* comme l'ennemi de la vie privée.

Elle exige simplement la mention d'un avertissement préalable dans les conditions générales du site (http://www.cnil.fr/index.php?id=1316). Bien entendu, les impératifs de déclaration préalable s'appliquent aux *cookies* comme à toute forme de traitement de données nominatives. Mais sur le droit d'acceptation du *cookie*, rien n'a été dit par le législateur.

Une seule parade contre le *cookie* : les effacer tous à chaque fois que vous changez de site Internet, pour éviter le profilage. Et bien entendu, à chaque fin de navigation.

b. Les traces laissées sur les serveurs

Tous les serveurs d'une entreprise connectés à l'Internet conservent des traces des connexions des salariés. On peut conserver (sans mouchard) un certain nombre d'informations telles que le nom de l'hôte de destination, les octets envoyés, le journal de connexions, les ports de destination et bien entendu, les adresses IP des sites consultés.

Par exemple, dans l'affaire *Lucent* contre la société d'autoroutes *Escota*, affaire de contrefaçon de marque et de diffamation sur l'Internet, un salarié de la société *Lucent* qui avait mis en ligne un site Internet injurieux et diffamatoire, déguisant la marque *Escota* en *Escroqua* et ayant contrefait le logo de la société d'autoroute, s'était connecté de son poste de travail dans l'entreprise pour mettre en ligne son site. Il a laissé toutes ces traces sur le serveur de *Lucent*. Ces données ont permis de l'identifier comme auteur de l'infraction - et ce, sans aucune difficulté.

2. Les traces envoyées de notre plein gré

C'est dans le cadre du commerce en ligne que ce type de preuve est le plus important. En effet, le consommateur est en situation de faiblesse par rapport à la conservation de la preuve. Par exemple, le cyber-commerçant en ligne doit indiquer le jour de conclusion du contrat électronique et laisser ce document à la disposition du consommateur. Le moment de conclusion du contrat constitue le point de départ du délai de livraison. Le consommateur a deux, voire trois, possibilités de conservation de la preuve. Il ne peut qu'imprimer le document contractuel en ligne, l'accusé réception envoyé par email, ou faire des captures d'écran c'est à dire sauver des images numériques.

Il est utile de noter néanmoins que le commerçant est tenu, au titre de l'article 1369-2 du Code civil introduit par la Loi pour la Confiance dans l'Economie Numérique[4], d'envoyer un accusé réception sous la forme d'un courrier électronique.

Cependant, face aux difficultés fréquemment rencontrées par le consommateur avec les commerçants en ligne, notamment quant aux délais de livraison, il serait nécessaire de se constituer une véritable

4 LCEN, Loi n°2004-575 du 21 juin 2004 JO du 22 juin 2004.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>

preuve numérique. En réalité, le consommateur doit se reposer sur des preuves plus traditionnelles : impressions d'écran, relevés bancaires, à défaut de pouvoir utiliser une véritable signature électronique.

II. Les insuffisances techniques de la preuve numérique

Face aux insuffisances de la preuve numérique actuelle dans la pratique française, un petit rappel sur l'échec de la mise en place d'une preuve avancée est nécessaire, avant d'aborder la question nouvelle de la biométrie comme mode de preuve numérique avancée.

A. Le cauchemar de l'industrie cryptographique en France

1. Une invention tout droit sortie d'un roman de science fiction : la carte à puce

Invoquons à présent le roman « La nuit des temps », de René Barjavel.

A Gondawa, société imaginaire décrite par Barjavel, la clé portée par les Gondas véhicule leur identité et sert de double virtuel sans lequel il n'est pas possible d'exister à Gondawa. La fuite d'Eléa, l'héroïne, à la fin du roman, illustre bien la difficulté de se soustraire à cette société parfaite en apparence, mais qui ne tolère pas la fraude ou l'exception.

A Gondawa « *Chaque fois qu'un Gonda désirait quelque chose de nouveau, des vêtements, un voyage, des objets, il payait avec sa clé. Il pliait le majeur, enfonçait sa clé dans un emplacement prévu à cet effet et son compte, à l'ordinateur central, était aussitôt diminué de la valeur de la marchandise ou du service demandés* ».

La clé de Gondawa sert aussi d'identifiant biométrique et biologique : c'est l'ordinateur central qui crée les couple par la « Désignation ». « - *La Désignation, qu'est-ce que c'est ? (...) - L'ordinateur central possède toutes les clés, de tous les vivants de Gondawa, et aussi des morts qui ont fait les vivants. Celles que nous portons ne sont que des copies. Chaque jour, l'ordinateur compare entre elles les clés de sept ans. Il connaît tout de tous. Il sait ce que je suis, et aussi ce que je serai. Il trouve parmi les garçons ceux qui sont et qui seront ce qu'il me faut, ce qui me manque, ce dont j'ai besoin et ce que je désire. (...) L'ordinateur a retrouvé les deux moitiés et les rassemble* ».

Ce concept d'identité biologique ou génétique est bien connu des sociologues qui s'interrogent sur la « crise d'identité » actuelle. Pour Claude Dubar, par exemple, si « *le patrimoine génétique, la biologie, permettent d'avoir une certaine stabilité dans la définition de soi, il ne s'agit en réalité que d'une illusion, car la définition de soi, dépend des autres* »[5].

Sommes nous si éloignés de cette univers de science fiction, créé en 1966 par René Barjavel sur une idée d'André Cayatte, le metteur en scène. Le concept véhiculé par la clé de Gondawa, clé universelle d'identification et d'authentification est très proche bien sûr, de la carte à puce inventée en 1974 par Roland Moreno.

Si Roland Moreno a toujours refusé d'attribuer la paternité de l'invention[6] ou tout au moins l'idée, au livre de Barjavel, Michel Ugon en revanche, alors directeur technique et industriel chez *Bull*-CP8, cite bien « La Nuit des temps » dans un article du numéro 176 de « *La Recherche* » (avril 1986) en attribuant à Barjavel la paternité de l'idée.

La carte à puces - avec le développement des technologies sans contact - se rapproche de plus en plus du concept de « clé universelle ».

Dans la carte sans contact, ni la puce ni l'antenne radio ne sont visibles. Ces cartes peuvent réaliser des transactions de façon beaucoup plus rapide que les cartes « contacts ». On peut par exemple, les laisser dans sa poche. Un bon exemple est celui du forfait dans les stations de ski. La société *Skidata*, société allemande rachetée par *Gemplus* en 2000, a développé cette technologie.

---

5 Cité des Sciences, Paris, Exposition « Le corps identité ».

6 Voir la page secrète de Roland Moreno, 23 mai 2002, <http://www.transfert.net/i8481>, rectificatif au livre publié « La Carte à Puce - Histoire Secrète », L'Archipel, 2002.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>

Un autre exemple dérivé de cette invention est celui des étiquettes radio, appelées « *tags* » en anglais ou encore RFID (*radio frequency identification*) qui peuvent être lues à quelques mètres. Ces étiquettes sont des marqueurs composés d'une antenne radio et d'une puce électronique. Leur taille est infime et leur masse négligeable. Ces étiquettes permettent de marquer toutes sortes d'objets et même des animaux. Les RFID sont accusés d'être des espions, tant ils sont faciles à dissimuler et ses usages potentiels variés.

Malgré la multiplicité des techniques disponibles, la signature électronique avancée, destinée à parfaire un système basé sur l'identité entre écrit papier et électronique n'a pas connu l'essor escompté. Le lobby français de la carte à puce avait pourtant réussi à imposer son standard, basé sur la cryptographie à clé publique et consacré dans le décret d'application de cette loi. La guerre larvée à l'époque entre l'industrie du logiciel et celle de la carte à puce, avait pour enjeu l'authentification sur l'Internet.

Il est étonnant que l'Etat français se réveille aujourd'hui seulement en prenant conscience de l'intérêt de la nation à voir rester française cette technologie de pointe[7]. En outre, couplée avec la biométrie, la carte à puce devient un élément de la sécurité intérieure.

Mais les fantastiques développements de la carte à puce n'ont pas réussi cependant à s'imposer comme outil de signature électronique.

2. L'impossible signature électronique

Un bref rappel s'impose, le texte ayant été largement commenté lors de son adoption et depuis lors.

« *Lorsqu'elle est électronique, (la signature) consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.* » (Code civil art. 1316-4).

Le décret d'application du 30 mars 2001 instaure une signature électronique sécurisée.

La loi française de transposition de la directive de 1999 sur les signatures électroniques a donc mis en place un cadre juridique totalement dépendant de la technique utilisée.

Le décret du 30 mars 2001 sera finalement complété par un décret du 18 avril 2002, qui met en place tout un système reposant sur le « certificat électronique » : soit un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.

Le certificat électronique qualifié répond à certaines exigences limitativement énumérées par le texte. Enfin ce système repose sur l'accréditation des tiers certificateurs. L'arrêté du 31 mai 2002[8] reconnaît au *Comité français d'accréditation* (COFRAC), le pouvoir d'accréditer les organismes qui procèdent à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification.

Les certificats sont largement utilisés par les commerçants en ligne. Par exemple, le protocole « *Secure Sockets Layer* (SSL) » sécurise les sites Web grâce au cryptage des informations et à la fourniture d'une authentification basée sur la fourniture d'un certificat par un tiers de confiance.

Mais aucun procédé de signature électronique avancée, accessible au consommateur et diffusé largement pour être utilisé dans le commerce électronique, n'a eu le soutien des banques ni de la grande distribution.

7 Les Etats-Unis intéressés par la biométrie de Gemplus, Le Monde Informatique, 4 juillet 2005, <http://www.lemondeinformatique.fr/actualites/lire-les-etats-unis-interesses-par-la-biometrie-de-gemplus-651.html>.

8 Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>

Compte tenu de ces échecs, outre les critiques à l'encontre de la fiabilité des algorithmes de chiffrement reposant sur la factorisation des nombres premiers, la biométrie a fait une irruption plutôt brutale avec le passeport et la carte d'identité biométrique, à la suite des attentats du 11 septembre.

B. La biométrie dans le droit français, freins culturels et nécessaire réforme législative ?

La généralisation de la biométrie, y compris dans le grand public a été brutale et le droit n'y était pas préparé. Mais avant de décrire le cadre juridique de la biométrie, quelques définitions sont nécessaires, suivies de réflexions.

1. Quelques définitions et réflexions

a. Qu'est ce que la biométrie ?

Suivant le rapport « *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en oeuvre* », rendu par le député Christian CABAL, la biométrie recouvre « *les techniques permettant d'identifier une personne à partir de l'un ou plusieurs de ses caractères biologiques ou comportementaux*[9] ». Le terme étant par ailleurs un mot dérivé de l'anglais « *biometrics* » introduit dans le vocabulaire scientifique au dix-neuvième siècle.

Un « **système biométrique »** devient donc une application technologique « *permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'oeil, contour de la main...), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche)*[10] ».

« *Les **données biométriques** constituent les informations à caractère morphologique, biologique ou comportemental propres à une personne. Il y a quelques années à peine, la technologie permettant de mesurer une diversité de caractéristiques biométriques et de les utiliser à des fins d'identification était relativement peu développée – hormis la technologie relative aux empreintes digitales, la plus courante et la plus ancienne. Aujourd'hui, aucun caractère biométrique ne semble exclu a priori et n'importe quelle caractéristique personnelle semble pouvoir se prêter à une mesure (à un niveau de fiabilité variable, cependant) par la technologie biométrique : différentes parties du corps, la voix, le geste, l'odeur, la chaleur corporelle, etc.* » [11].

Les dispositifs biométriques permettent tour à tour d'identifier ou d'authentifier une personne. Ceci représente une différence majeure. Le contrôle d'accès physique à un bâtiment jugé sensible nécessite que l'on soit identifié.

Sur l'Internet en revanche, pour des besoins ne répondant pas à un impératif de sécurité, nous n'avons besoin que d'être authentifiés : l'identification ne serait qu'un processus ultérieur, rendu possible en cas de fraude (on peut être authentifié par exemple, avec un pseudonyme).

b. Réflexions

Dans nos sociétés démocratiques, il y a bien une porte ouverte à certains types de fraude. Tout n'est pas contrôlé. Cette conception humanitariste est cependant remise en cause. Pour ne citer qu'un exemple : récemment, une fraude à la sécurité sociale a été commise par une femme ayant enregistré dix-sept fois aux allocations familiales des triplés qui n'existaient pas, pour toucher des allocations. Ces failles dans le système sont de moins en moins tolérées par l'opinion publique.

9 Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en oeuvre, *Office parlementaire d'évaluation des choix scientifiques et technologiques*, Christian CABAL, député, Sénat, Assemblée nationale (France), juin 2003, p. 7, <http://www.assemblee-nationale.fr/12/dossiers/030938.asp>.

10 Définition de la *Commission nationale de l'informatique et des libertés* (CNIL – France), rapportée dans *Office parlementaire d'évaluation des choix scientifiques et technologiques*, Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en oeuvre, Christian CABAL, député, Sénat, Assemblée nationale (France), juin 2003, p. 7, note 6, p. 8.

11 *Commission de l'éthique de la science et de la technologie*, (Canada) L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques, Document de réflexion, décembre 2004 <http://www.europeanbiometrics.info/images/resources/97_542_file.pdf>, Diane Duquet, coordonnatrice.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>

Pourtant, il est facile d'imaginer une société dans laquelle l'individu existe grâce à son identité enregistrée dans une machine. Dans les années 60, le projet du gouvernement de donner un numéro à chaque citoyen souleva un tollé tel qu'il fut abandonné. **La biométrie est une façon détournée de revenir à cet identifiant unique.**

Il reste à savoir - hormis les considérations sociologiques et philosophiques - si cette technique peut nous faciliter la vie ou au contraire, l'empoisonner.

Au Canada, le *Commissariat à la protection de la vie privée* a émis quatre critères ayant pour but de déterminer les répercussions des technologies biométriques et d'autres mesures de sécurité sur la vie privée :

1 - la mesure est manifestement nécessaire pour répondre à certains besoins ;

2 - tout indique que la mesure sera probablement efficace pour satisfaire les besoins à l'origine du déploiement proposé ;

3 - l'ingérence dans la vie privée est proportionnelle à l'avantage en matière de sécurité ;

4 - il peut être montré qu'aucune autre mesure comportant une ingérence moindre dans la vie privée ne permettrait pas d'atteindre les mêmes résultats.

Ce n'est pas du tout cette orientation qui a été prise en France, puisque des systèmes biométriques sont de plus en plus utilisés y compris lorsqu'ils pourraient manifestement être remplacés par un autre système. C'est le cas pour les cantines scolaires à l'école primaire.

2. Cadre juridique

a. Genèse de l'encadrement de la biométrie par le droit français

Plusieurs contradictions peuvent être relevées dans l'encadrement juridique actuel de la biométrie. La directive 95/46/CE [12] 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 rappelle dans son considérant numéro deux : « *que les systèmes de traitement de données sont au service de l'homme; qu'ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus* ».

L'article 6 dispose 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* ».

Pour autant, ces objectifs louables ne sont pas pris en compte dans la procédure française. C'est en effet en vertu de cette directive que tout naturellement en France, la CNIL a été investie des pouvoirs de contrôle et d'autorisation de traitements de données biométriques, par la loi n° 2004-804 du 6 août 2004. C'est le principe de l'autorisation préalable qui a été retenu.

Mais la CNIL apprécie de façon plutôt légère, le principe de finalité exposé ci-dessus. Aux fins de transposition de la directive, la loi de 2004 a opéré une substitution entre les « *données nominatives* » de la loi de 1978 par « *les données à caractère personnel* » qui répondent mieux aux exigences des nouvelles techniques employées (art. 2).

12 <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&an_doc=95&nu_doc=46>.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>

La CNIL a très récemment rendu trois décisions accordant des autorisations aux traitements utilisant certains gabarits, suivant leur finalité[13].

Cette sorte d'exemption par catégorie (en référence au droit communautaire de la concurrence) permet de faire une simple déclaration de son traitement.

b. Les autorisations par catégories de traitement biométrique

La CNIL a adopté une position suivant laquelle la biométrie ne peut servir qu'à authentifier une personne lorsque aucun impératif de sécurité n'est en cause. Dans trois décisions du **27 avril 2006**, elle a accordé des exemptions d'autorisation à certaines catégories de traitement biométrique. Il s'agit des systèmes utilisant - le **contour de la main** pour le contrôle d'accès, la gestion des horaires et de la restauration sur les lieux de travail ; - **l'empreinte digitale exclusivement enregistrée sur un support individuel** pour le contrôle de l'accès aux locaux sur les lieux de travail ; - le contour de la main pour l'accès au restaurant scolaire.

L'utilisation de l'empreinte digitale comme gabarit dans un système biométrique n'a la faveur de la CNIL que lorsque le support de l'empreinte est conservé sur soi et non dans une base de données centralisée. Cette dernière pourrait en effet être utilisée à d'autres fins. En outre, il est possible de collecter les empreintes sans le consentement de la personne, puisque les empreintes sont laissées partout dans les actes de la vie quotidienne.

La conservation des gabarits sur un support individuel, ou l'utilisation de gabarits qui ne laissent pas de traces, tels que la reconnaissance du contour de la main ou de l'iris, est donc préférée par la CNIL aux autres systèmes.

Dans une délibération n°04-018 du 8 avril 2004[14], la CNIL a refusé la mise en place par un hôpital, d'un dispositif biométrique basé sur l'empreinte digitale destiné à la gestion des horaires du personnel. La CNIL relève que : « *le surcroît de sécurité et les commodités d'usage qui sont attendues du recours aux techniques biométriques ont, le plus souvent, pour contrepartie l'enregistrement dans une base de données informatique des éléments physiques d'identification des personnes. Or, les empreintes digitales font partie des données biométriques qui laissent des traces pouvant être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou avoir en main. Aussi la constitution d'une base de données d'empreintes digitales est-elle susceptible d'être utilisée à des fins étrangères à la finalité recherchée par sa création (...). Aussi le traitement pris dans son ensemble n'apparaît-il ni adapté ni proportionné à l'objectif poursuivi* ».

Poursuivant la même logique, la CNIL a autorisé un système d'identification biométrique pour l'accès à une cantine scolaire, basé sur la reconnaissance du contour de la main et a refusé d'autoriser un système d'empreintes digitales ayant le même objet[15]. La *Commission Informatique et Libertés* commente sa propre décision en soulignant : « *La technique du "contour de la main" retenue par le collège de Carqueiranne, à la différence de celle des empreintes digitales choisie par le collège de Nice, ne laisse pas de trace dans la vie courante et ne peut donc être détournée de sa finalité première.*

Par cet avis positif rendu en faveur d'une application biométrique basée sur le contour de la main, la Commission poursuit l'élaboration d'une doctrine qui encadre et accompagne le développement d'une nouvelle technologie dans le respect des libertés fondamentales ».

Ainsi, une solution technique vers laquelle tout le monde semblerait s'accorder - le CLUSIF, le *Forum des Droits sur l'Internet* et la CNIL - serait donc la combinaison de la biométrie et de la cryptographie à clé publique mise en oeuvre par exemple, dans une carte à puce conservée par l'utilisateur, pour l'identification avec l'empreinte digitale.

---

13 Biométrie : la CNIL encadre l'utilisation de certains dispositifs et simplifie leur déclaration, 18 mai 2006, Echos des séances, <http://www.cnil.fr/index.php?id=2019&news[uid]=349&cHash=01b1d0a219>.

14 Délibération n°04-018 du 8 avril 2004 : Cnil.fr, Délibération n°04-018 relative à une demande d'avis présentée par le Centre hospitalier de Hyères concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de ses personnels.

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

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>
Juriscom.net droit des technologies de l'information

Il est en effet possible d'inclure le gabarit de l'empreinte digitale dans une puce qui permet d'identifier un utilisateur en comparant un doigt placé sur un lecteur d'empreintes digitales avec l'empreinte stockée dans la carte.

Cependant, il paraîtrait raisonnable, qu'à l'instar du *Commissariat à la protection de la vie privée* du Canada, la CNIL se penche également sur le critère de nécessité du système biométrique et qu'il soit démontré qu'aucune autre mesure comportant une ingérence moindre dans la vie privée, ne permettrait d'atteindre les mêmes résultats. Beaucoup de systèmes coûteux, pas toujours efficaces ni nécessaires et constituant en outre une ingérance dans la vie privée, seraient ainsi évités.

Conclusion

Une évolution vers une identité virtuelle est la seule parade possible contre l'espionnage commercial de nos vies privées. Pas question en effet, de laisser surfer nos enfants qui laisseront au hasard du *web*, quantité de données récupérées par des sociétés commerciales, des agences gouvernementales comme aux Etats-Unis ou encore des pirates.

Loin d'être effrayée par la carte à puce sur Internet, je rêve d'une carte hautement sécurisée à insérer juste avant de surfer, qui ne permettra la divulgation d'informations seulement si je l'ai décidé et au besoin, induira en erreur les sites marchands en créant de faux profils ou des profils anonymes.

Chaque avancée technologique a un prix. La biométrie comme technique de preuve numérique y compris sur les réseaux, ne doit pas donner prétexte à une intrusion inacceptable dans nos vies privées. C'est une question essentielle qui devra tôt ou tard être débattue dans un cadre démocratique.

Nota :

Pour plus d'informations sur les traces laissées sur l'Internet : http://www.cnil.fr/index.php?id=19.

Citations et liens:

Remerciements à G.M. Loup, dont le travail de documentation publié sur sa page web et relatif à la comparaison entre le roman de Barjavel et la génèse de la carte à puces est très intéressant : http://barjaweb.free.fr/SITE/ecrits/Ndt/nuit.php#sommaire.

Exposition „Biométrie, le corps identité, Cité des sciences et de l'industrie, Paris, http://www.cite-sciences.fr/francais/ala_cite/expositions/biometrie/index2.php.

La biométrie vue par le Droit européen, http://www.europeanbiometrics.info/activities/index.php.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>

Sommaire

S. M.

Copyright © Séverine MAS
Juriscom.net, 1er mars 2007, <http://www.juriscom.net>