Généralisation des capteurs d'empreinte digitale et risques d'atteintes à la vie privée

publié le **21/10/2013**, vu **10373 fois**, Auteur : Anthony BEM

Comme en témoigne le système d'authentification par empreinte digitale intégré dans le dernier téléphone d'Apple : l'Iphone 5S, la reconnaissance des empreintes digitales est devenue une technique en passe de se généraliser qui soulève des questions d'ordre juridique, en raison notamment des risques éventuels d'atteintes à la vie privée et à la protection des données à caractère personnel et d'usurpation d'identité.

Pour mémoire, une empreinte digitale correspond à la trace laissée par le bout d'un doigt sur un support et dont le dessin résulte des fins plissements présents sur la peau du doigt et appelés crêtes papillaires.

Les empreintes digitales se forment très tôt chez l'embryon, restent inchangées durant toute la vie et sont différentes chez chacun d'entre nous et donc uniques, même chez les vrais jumeaux.

Ainsi, en 1892, le scientifique Francis Galton a estimé qu'il y a 1 chance sur 64 milliards pour que deux personnes aient les mêmes empreintes digitales.

Ce caractère unique des empreintes digitales explique le rôle particulier que jouent ces dernières dans le domaine de l'identification des personnes en général.

En effet, depuis longtemps, dans le cadre d'enquêtes criminelles, la comparaison des empreintes digitales prélevées sur un lieu avec celles stockées dans une base de données permet d'établir la présence sur ce lieu d'une certaine personne.

Les empreintes digitales sont également utilisées pour vérifier l'authenticité d'un passeport et l'identité de son titulaire, dans le but de limiter les risques de falsification.

Mais, si au départ l'empreinte digitale n'était utilisée que par la police scientifique ou l'administration, aujourd'hui elle s'est généralisée.

Les systèmes de reconnaissance par empreinte digitale s'invitent en effet de plus en plus dans notre quotidien.

On les trouve déjà dans les aéroports, dans certaines entreprises et même dans des supermarchés.

En outre, de plus en plus d'appareils électroniques tels que les ordinateurs et les téléphones portables intègrent un dispositif de reconnaissance par empreinte digitale.

En témoigne l'Iphone 5S d'Apple qui intègre un système de reconnaissance par empreinte digitale baptisé Touch ID.

Le tout nouveau appareil téléphonique HTC « One Max » comporte également un lecteur d'empreintes digitales capable de déverrouiller l'appareil sans code de sécurité et de lancer

automatiquement jusqu'à trois actions distinctes en attribuant une empreinte de doigt différente à chacune d'elles.

Les capteurs d'empreinte digitale offrent des avantages en termes de facilité, de confort, de sécurité et de rapidité de l'identification d'une personne.

Ainsi, il n'est plus besoin de retenir un mot de passe ou de transporter des clés ou des cartes de paiement lorsque l'on peut utiliser son propre doigt pour accéder aux locaux de certaines entreprises par exemple ou procéder à un paiement dans certains supermarchés.

Cependant, force est de constater que la généralisation des systèmes de reconnaissance par empreinte digitale n'est pas sans poser des questions d'ordre juridique.

En effet, parce que l'empreinte digitale est une donnée personnelle, la généralisation de son utilisation engendre des risques d'atteintes aux droits au respect de la vie privée et à la protection des données à caractère personnel.

Ces risques sont d'autant plus élevés que près de 45% de la population française utilise un smartphone et qu'en l'état actuel des choses, l'intégration de systèmes de reconnaissance par empreinte digitale dans des téléphones portables n'est pas soumise à la loi Informatique et Libertés qui exige l'autorisation de la CNIL.

Pour mémoire, la loi Informatique et Libertés du 6 janvier 1978 est applicable dès lors qu'il existe un traitement par un tiers des informations personnelles relatives à des personnes physiques.

Autrement dit, il faut en principe que deux conditions soient remplies pour que cette loi s'applique : d'une part, des données à caractère personnel ; d'autre part, un traitement de ces données par un tiers.

S'agissant de la première condition, elle est satisfaite par les empreintes digitales, dans la mesure où ces dernières constituent des données à caractère personnel.

Une donnée à caractère personnel est définie comme une information relative à une personne physique identifiée ou qui peut être identifiée par référence à un ou plusieurs éléments qui lui sont propres.

Ces éléments concernent donc aussi bien les informations directement nominatives telles que le nom et le prénom, que les éléments du corps humain tels que l'empreinte digitale.

Comme l'a affirmé la Cour européenne des droits de l'homme, les empreintes digitales constituent des données à caractère personnel car elles se rapportent à des individus identifiés ou identifiables. (CEDH, 4 décembre 2008, requêtes n° 30562/04 et 30566/04, Affaire S. et Marper c/ Royaume-Uni).

Dans le même sens, la Cour de justice de l'Union Européenne a récemment considéré que :

> « *Le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel se rapporte à toute information concernant une personne physique identifiée ou identifiable.*

> ***Les empreintes digitales relèvent de cette notion dès lors qu'elles contiennent objectivement des informations uniques sur des personnes physiques et permettent leur identification précise*** » (CJUE, 17 octobre 2013, n° C-291/12, Michael Schwarz c/ Stadt Bochum)

Ainsi, les empreintes digitales constituent sans nul doute des données à caractère personnel et remplissent donc la première condition d'application de la loi Informatique et Libertés.

Cependant, s'agissant de la deuxième condition relative au traitement des données par un tiers, elle fait défaut dans le cas précis de l'intégration de système de reconnaissance par empreinte digitale dans l'Iphone 5S.

En effet, constitue un traitement de données à caractère personnel toute opération appliquée par un tiers à ces données, telle que leur collecte, leur enregistrement, leur conservation, leur consultation ou leur utilisation.

En l'occurrence, concernant l'Iphone 5S, Apple déclare que les scans des empreintes digitales ne sont pas confiés à un tiers mais sont conservées au sein même du téléphone, lequel demeure la possession exclusive de son propriétaire.

L'un des responsables d'Apple, Dan Riccio, a en effet précisé que « *toutes les informations sont encryptées au cœur du téléphone, dans l'enclave sécurisée de la puce A7, seulement accessible par Touch ID et ne seront jamais disponibles à d'autres logiciels, jamais stockées sur les serveurs d'Apple ni sauvegardées sur iCloud* ».

Dans ces conditions, on ne saurait parler de traitement par un tiers à propos du capteur d'empreintes digitales intégré dans l'Iphone 5S, dans la mesure où les scans des empreintes digitales sont cryptés et conservés sur la puce du téléphone exclusivement détenu par la personne concernée qui a ainsi la maîtrise de sa donnée biométrique.

De ce fait, l'empreinte digitale reste sous la responsabilité du propriétaire de l'Iphone 5S et ne peut pas être utilisée pour l'identifier à son insu, de sorte que l'autorisation de la CNIL n'est pas nécessaire.

Cependant, si les scans d'empreintes digitales ne devaient plus être conservés sur la puce de l'Iphone 5S mais sur des serveurs distants ou s'ils venaient à faire l'objet d'un traitement automatisé par des logiciels, cela pourrait multiplier les risques de violation de la vie privée et dans un tel cas l'intervention de la CNIL serait nécessaire.

Pour le moment, le fait que les scans d'empreintes digitales soient stockés sur un support individuel, à savoir la puce du téléphone, atténue donc les risques d'atteintes à la protection des données à caractère personnel, car celles-ci échappent au traitement par un tiers.

De nombreuses autres questions restent néanmoins en suspens, notamment sur le niveau de sécurité du système de reconnaissance par empreinte digitale.

En effet, comme nous le verrons dans un prochain article, ces systèmes d'identification ne sont pas à l'abri de piratage et n'excluent pas les risques d'usurpation d'identité.

Je suis à votre disposition pour toute action ou information (en cliquant ici).

PS : Pour une recherche facile et rapide des articles rédigés sur ces thèmes, vous pouvez taper vos "*mots clés*" dans la barre de recherche du blog en haut à droite, au dessus de la photographie.

Anthony Bem
Avocat à la Cour
27 bd Malesherbes - 75008 Paris
Tel : 01 40 26 25 01

Email : abem@cabinetbem.com

www.cabinetbem.com