Les risques juridiques des logiciels de reconnaissance faciale

publié le **01/10/2014**, vu **5295 fois**, Auteur : Murielle Cahen

Les logiciels de reconnaissance faciale ont aujourd'hui gagné en performance et en fiabilité. Les plus avancés peuvent ainsi travailler avec des images de base qualité telles que celles fournies par les caméras de vidéosurveillance. Cette technologie, de plus en plus présente dans nos vies, inquiète et pose de véritables problèmes d'atteinte à la vie privée.

Depuis leur apparition dans les années 1990, les logiciels de biométrie sont devenus de plus en plus performants notamment en terme de rapidité de traitement et de fiabilité. Comment fonctionne ce procédé ? Le visage est capturé à l'aide de n'importe quel capteur, caméra ou appareil photo, et l'image est ensuite traitée par un logiciel qui repère en général la position des yeux pour procéder à un alignement.

Grâce à cela, le logiciel fait un relevé des différents points caractéristiques du visage (nez, sourcils, écartement des yeux etc.). Ces informations sont codées sous forme de fichier, le gabarit, dans lequel s'effectueront les recherches. Il est ensuite possible de repérer les similitudes entre les captures de visage et les gabarits présents en base de données. Avant même la naissance de la technologie, ce procédé était utilisé par la police grâce à la technique du bertillonnage ; technique criminalistique mise au point par Alphonse Bertillon en 1879 et reposant sur l'analyse biométrique accompagnée de photographies de face et de profil.

Le principe était de réaliser des mesures sur les criminels, de noter entre autre l'écartement entre les yeux, la taille du visage, les oreilles… afin de réaliser un fichier d'identification permettant de les reconnaître plus facilement en cas de nouvelle arrestation. Aujourd'hui, les technologies utilisent les mêmes techniques grâce à un algorithme qui permet de comparer un visage à une photo de sa base de donnée.

Jugées peu fiables à l'époque, elles permettent dorénavant un taux de rejet de plus en plus faible. Les réseaux sociaux ont profondément contribué à cette évolution et tous les géants technologiques se sont appropriés ce savoir-faire d'identification des visages. Le logiciel d'Apple « iphoto », l'application « Picassa » et le réseau social Facebook utilisent tous ce système de reconnaissance faciale. Le paradoxe de Facebook résulte dans le fait que ce sont les utilisateurs eux-mêmes qui abreuvent chaque jour le réseau de centaines de millions de photographies. Selon ce dernier, 100 millions de noms sont mis en légende sous des visages quotidiennement. Mais alors, quid des craintes sur le respect de la vie privée, sur la possibilité que la police utilise ce système pour mener des enquêtes illégales ou pour que des gens malintentionnés s'en servent à mauvais escient ? Ces inquiétudes sont non seulement légitimes mais laissent également penser à quel point cette technique nécessite un encadrement pour éviter les dérives.

I- Logiciels biométriques et risques d'atteinte à la vie privée

A) Le droit à l'image

Grâce à ces techniques, les visages ont été transformés en données électroniques qu'il est désormais possible de regrouper, d'analyser et de classer. Or, ces données sont sensibles et précieuses car elles sont une caractéristique de notre corps et un élément de notre identité. Certaines utilisations de la reconnaissance faciale sont incontestablement bénéfiques notamment en ce qui concerne l'authentification des employés autorisés à avoir accès à une centrale nucléaire ou la lutte contre la fraude visant les individus qui présentent des demandes de passeport sous différents noms.

Mais, la reconnaissance faciale a également des répercussions sur le respect de notre vie privée et certains auteurs estiment que cette technologie signe la fin de l'anonymat. La base de données d'images de Facebook est certainement la plus importante au monde. Sur ce réseau planétaire, l'utilisateur a notamment la possibilité de « taguer » une photographie pour y associer un nom et un profil.

En 2011, Facebook lance un système de reconnaissance faciale qui permet, à partir d'un nom, de retrouver sur le réseau et le web, toutes les images représentant la personne. Ce système a été abandonné par Facebook pour l'Europe en septembre 2012 à la suite d'une série de plaintes déposées par un étudiant autrichien, Max Schrems, devant l'autorité irlandaise chargée de la protection des données privées. Parmi les projets en développement, Facebook va frapper fort avec son programme de recherche DeepFace qui sera dévoilé en détail à la fin du mois de juin. La société qui possède 250 milliards de photos personnelles pourra bientôt identifier tout un chacun avec son système de reconnaissance faciale. Ce système ne devrait pas être destiné aux utilisateurs.

B) Utilisation des données personnelles et sécurisation des données

Se pose également la question de la sécurisation des données en ligne. L'application Snapchat, prisée par les jeunes car elle promet l'autodestruction des photos partagées en quelques secondes, a admis de graves failles. Accusée d'avoir récolté les carnets d'adresses des utilisateurs sans leur consentement et de les avoir trompé sur la disparition des fichiers échangés, l'application Snapchat qui n'avait pas sécurisé sa base d'utilisateurs a été victime de pirates qui ont pu récupérer noms et numéros.

Par ailleurs, une application actuellement en deuxième période d'essai nommée NameTag fonctionne sur les Google Glass et permet de scanner n'importe quelle personne dans la rue puis de l'envoyer vers les serveurs de FacialNetwork afin de dresser une comparaison avec une base de données contenant pour le moment 2,5 millions de portraits. Après une analyse par le logiciel, le nom de la personne est présenté avec la possibilité de consulter les informations rendues publiques sur divers réseaux sociaux communautaires tels que Facebook, Twitter, LinkedIn ou Instagram. La société dispose également de 450 000 fiches issues de la base américaine des agresseurs sexuels et autres criminels.

Pour ses lunettes, Google a strictement interdit les applications de reconnaissance faciale reconnaissant la violation de la vie privée. En matière de police judiciaire les avancés permises par ces logiciels sont certaines. En 2012, le FBI avait investi un milliard de dollars dans ce qui devait être un « programme d'identification de nouvelle générateur » permettant de constituer une base de données nationale photographique des criminels puis quelques informations concernant leurs données biométriques A l'époque, les défenseurs de la vie privée s'inquiétaient déjà que des personnes au casier vierge et non suspectes puissent figurer dans ce fichier et se retrouver surveillées.

Cette crainte semble aujourd'hui se justifier d'après des documents récupérés par la Fondation Electronic Frontier, une ONG a but non lucratif, selon lesquels 4,3 millions de clichés ont été récupérés sans aucune implication criminelle ou enquête en cours. On peut donc imaginer plusieurs situations : celle dans laquelle un innocent se retrouve au cœur d'une enquête criminelle, mais aussi celle où la technologie est utilisée à mauvais escient pour atteindre d'autres objectifs visés par les pouvoirs publics notamment pour réprimer la dissidence. La protection des données biométriques et leur vulnérabilité au piratage et aux utilisations malveillantes suscitent des inquiétudes.

II- La nécessité d'un encadrement afin d'éviter les dérives

A) Le contrôle de la CNIL en France

Selon une étude effectuée à la demande de la CNIL par TNS Sofres, les technologies de reconnaissance faciale qui permettent d'associer automatiquement un nom suscitent des inquiétudes pour 41% des participants, malgré une faible utilisation pour le moment (12% des internautes).

La CNIL est chargée d'encadrer les pratiques liées à la biométrie faciale. Face à cette technologie, un cadre légal est nécessaire. A moins d'avoir nommé un correspondant Informatique et Liberté (CIL), une déclaration auprès de la CNIL est nécessaire en cas d'usage de vidéosurveillance. Concernant les usages privés, la CNIL a surtout un rôle d'information générale et d'éducation des internautes quant à leur utilisation des réseaux sociaux.

Elle a émis plusieurs recommandations dans certains articles de son site afin de sensibiliser les citoyens sur ces pratiques et d'éviter les dérives. En France, la reconnaissance faciale appliquée à la sécurisation des accès dans les entreprises ou dans les lieux publics est soumise à l'autorisation de la CNIL. Si l'application est mise en œuvre pour le compte de l'Etat, il faut un décret en Conseil d'Etat après un avis préalable de la commission. Au contraire, si l'application biométrique est limitée à un usage exclusivement personnel, elle ne sera pas soumise à la loi Informatique et libertés (exemple : reconnaissance faciale qui sécurise l'accès aux ordinateurs domestiques, à un Smartphone).

Si en France nous sommes assez loin de la surveillance globale, il existe à New-York des caméras installées dans la ville qui permettent d'observer les citoyens et de pouvoir effectuer une analyse biométrique de leur visage afin de le comparer à une base de donnée dans un but de protection contre le terrorisme. L'idée que les autorités puissent identifier toute personne marchant dans la rue est inquiétante et attentatoire à la vie privée. La législation devra surement s'adapter avec l'arrivée de ces nouvelles technologies telles que les lunettes connectées ou encore les drones.

B) Rebondissements à l'échelle internationale

Des réflexions sur le sujet sont menées dans de nombreux pays. En mars 2012, le Groupe de travail « Article 29 sur la protection des données de l'Union européenne » a exprimé son opinion concernant la reconnaissance faciale dans les services en ligne et mobiles en vue d'une réflexion sur le cadre juridique approprié et de la formulation de recommandations.

Ce groupe de travail mentionne l'absence de consentement, les mesures de sécurité insuffisantes et le fait que ces technologies pourraient sonner le glas de l'anonymat. En avril 2012, le groupe de travail a rendu publique une opinion qui indique qu'il faut obtenir le consentement de l'intéressé pour stocker et utiliser des données biométriques. De ce fait, Facebook a été contraint de désactiver son système de reconnaissance faciale qui contrevenait aux lois sur la protection des données de l'UE et à supprimer les photos qu'il avait recueillies en Allemagne. La Federal Trade Commission est également intéressée par ces questions et a rendu publique des pratiques exemplaires (autorisation des clients) à l'intention des entreprises ayant recours aux technologies de détection des visages.

La reconnaissance faciale confère une nouvelle dimension à la surveillance du fait qu'elle permet d'identifier les individus beaucoup plus rapidement et aisément. Elle est clairement un des enjeux majeurs de ces prochaines années face au développement de ces nouvelles technologies et d'autant plus avec l'arrivée de la géolocalisation.

-

Sources :

- http://www.droitnumerique-sorbonne.fr/biometrie-faciale-la-fiction-aux-portes-de-la-realite.html#
- http://www.priv.gc.ca/information/research-recherche/2013/fr_201303_f.asp
- http://www.journaldugeek.com/2014/01/14/nametag-application-reconnaissance-faciale/
- http://moreas.blog.lemonde.fr/2011/11/01/notre-visage-enjeu-biometrique-de-demain/