Généralisation des capteurs d’empreinte digitale et risques de piratage et d’usurpation d’identité

publié le **28/10/2013**, vu **7430 fois**, Auteur : Anthony BEM

Face à la généralisation des systèmes de reconnaissance par empreinte digitale illustrée notamment par l’intégration d’un capteur d’empreinte digitale dans l’Iphone 5s, il est légitime de s’interroger sur les risques éventuels de piratage et d’usurpation d’identité et les conséquences juridiques qu’ils pourraient emporter.

Tel que nous avons déjà eu le plaisir de l'envisager dans un article précédent, les systèmes de reconnaissance par empreinte digitale sont en passe de se généraliser.

Si cette généralisation des capteurs d’empreintes digitales est aujourd’hui principalement incarnée par Apple et son nouveau Iphone 5S, de nombreuses autres grandes sociétés s’intéressent de plus en plus à la technologie de la reconnaissance par empreinte digitale.

Par exemple, des sociétés telles que Google, Paypal, Blackberry, Lenovo, LG Electronics, Mastercard se sont regroupées autour de l’alliance Fast IDentity Online (FIDO) dans le but de développer des solutions alternatives permettant d’authentifier les utilisateurs sans recourir aux mots de passe.

Parmi ces solutions alternatives figurent la reconnaissance par empreinte digitale considérée par l’alliance FIDO comme pouvant remédier aux problèmes de piratage et d’oubli de mots de passe.

Pour ce faire, l’alliance FIDO entend équiper le système Android de capteurs d’empreintes digitales pour faciliter l’utilisation de services en ligne et sécuriser les transactions en ligne.

Ainsi, selon l’alliance, les premiers téléphones Android intégrant des capteurs d’empreintes digitales seront commercialisés dans le courant de l'année 2014.

Un tel engouement pour la technologie de reconnaissance par empreinte digitale semble être suscité par notre besoin croissant de sécuriser nos informations privées.

Aux dires de certains, les capteurs d’empreinte digitale permettraient de se protéger contre les menaces d'atteinte au respect de la vie privée accentuées par l’essor d’internet et du commerce en ligne et la multiplication des applications en tous genres.

Ainsi, dans un contexte où l’utilisation des smartphones et le commerce électronique soulèvent de nombreuses préoccupations par rapport à la vie privée, les systèmes de reconnaissance par empreinte digitale constituent un sérieux argument commercial pour les fabricants de téléphones portables.

Cependant, si la technologie de la reconnaissance par empreinte digitale peut constituer un gage de sécurité, il faut bien reconnaitre que les utilisateurs d’appareils électronique intégrant une telle

technologie ne sont pas complètement à l'abri de violation de leur privée et d'usurpation de leur identité.

Par exemple, s'agissant de l'Iphone 5S, le fait que les scans d'empreintes digitales soient stockés sur la puce du téléphone est censé protéger les utilisateurs contre le risque de lecture et de vol de ces données personnelles par d'autres personnes.

Mais, une telle précaution ne garantit pas pour autant une sécurité absolue car les systèmes biométriques sont vulnérables au piratage, à plus forte raison lorsqu'ils impliquent une connexion sur internet.

En effet, sur la page descriptive des fonctionnalités de l'Iphone 5S, Apple déclare que «*votre empreinte vous permet également de confirmer vos achats sur l'iTunes Store, l'App Store et l'iBooks Store, ce qui vous évite d'avoir à entrer chaque fois votre mot de passe.*»

Or, l'utilisation des données biométriques à des fins de commerce électronique implique une connexion à internet et l'envoi de ces données pour confirmer l'identité de l'acheteur auprès du store concerné, ce qui les expose au risque d'être interceptées ou détournées par des personnes mal intentionnées.

En outre, en prévoyant la possibilité d'utiliser son empreinte digitale pour confirmer des achats auprès de ses stores, Apple pourrait bien ouvrir une nouvelle ère dans l'utilisation de données biométriques à des fins commerciales.

Cela est d'autant plus probable que Tim Cook, directeur général d'Apple, n'exclut pas que puissent être « *imaginés de nombreux autres usages dans le futur* ».

De même, même si Apple assure que les données biométriques sont cryptées et stockées sur le processeur de l'Iphone, on peut craindre que les empreintes digitales numérisées puissent un jour être accessibles par d'autres entreprises qui pourraient s'en servir pour un autre usage que celui pour lequel ils les ont recueillies initialement.

En effet, avec les avantages en termes de sécurité, de rapidité et de confort qu'offre l'empreinte digitale, celle-ci est susceptible d'intéresser de nombreux sites internet et services en ligne qui pourraient s'en servir par exemple à des fins de marketing ou de publicité en ligne ciblée, sans en informer les personnes concernées.

Comme le soutient Johannes Caspar, membre de la CNIL allemande, « *l'utilisateur-moyen d'un Iphone est incapable de vérifier, au niveau technique, ce qui se passe avec son empreinte lorsqu'elle est sur l'Iphone. Il ne peut pas dire avec certitude ou avec facilité à quels types de données privées les applications téléchargées sur l'Iphone ont accès. La révélation récente de programmes d'espionnage comme PRISM font qu'il est plus risqué que jamais de partager des informations personnelles importantes sur un appareil électronique.* »

Une éventuelle transmission des données biométriques est donc à craindre, surtout que les détenteurs d'Iphone 5S pourraient de ce fait perdre la maîtrise de leurs empreintes digitales qui seraient ainsi détenues par des tiers, ce qui accentuerait les risques de violation de vie privée et d'usurpation d'identité.

Par ailleurs, on peut aussi craindre un risque de piratage des capteurs d'empreinte digitale.

En effet, parmi les systèmes biométriques, l'empreinte digitale présente la caractéristique d'être une biométrie à trace, dans la mesure où chacun laisse des traces de ses empreintes digitales dans de nombreuses circonstances de la vie courante, comme sur un verre ou une poignée de

porte.

Or, ces traces, plus ou moins exploitables, peuvent être capturées à l'insu des personnes concernées et il peut en résulter des risques de dérive.

L'exemplaire de l'empreinte relevé peut par exemple être utilisé pour procéder à l'identification d'une personne à son insu ou pour usurper son identité en utilisant l'exemplaire de l'empreinte récupéré pour frauder un dispositif reposant sur la reconnaissance de l'empreinte digitale.

Ces risques sont d'autant plus élevés que les traces digitales laissées par une personne sur un support sont nombreuses comme le sont les techniques pour les relever.

Ainsi, en 2002, un chercheur japonais était parvenu à démontrer qu'il est possible de pirater un lecteur d'empreintes digitales à l'aide de gélatine, comme celle contenue dans les bonbons.

Plus récemment, d'après une information rapportée par plusieurs journaux et sites d'informations, un groupe de hackers allemands dénommé le Chaos Computer Club a déclaré avoir réussi à pirater le système de reconnaissance par empreinte digitale intégré dans l'Iphone 5s à peine quelques jours après son lancement.

Sur son site internet, le Chaos Computer Club a expliqué être arrivé « *par des moyens simples de tous les jours* » à hacker le lecteur d'empreintes digitales d'un IPhone 5S sans utiliser le doigt de son propriétaire.

Avec une vidéo à l'appui, le groupe de hackers a détaillé la procédure qui a consisté :

- d'abord, à récupérer l'empreinte du propriétaire du smartphone sur une surface transparente telle qu'une bouteille en verre ;

- puis, à l'aide d'un système d'impression laser, à reproduire cette empreinte sur une surface transparente sur laquelle ils ont appliqué un dérivé du latex ;

- enfin, à humidifier l'empreinte recréée avant de l'apposer sur la cellule du téléphone.

On comprend dès lors que la généralisation des capteurs d'empreinte digitale doit inciter à la plus grande prudence en raison des risques qu'elle fait peser sur l'identité des personnes possédant des téléphones portables les intégrant.

Une telle prudence est d'autant plus nécessaire que l'usurpation d'identité qui pourrait résulter du piratage d'un capteur d'empreinte digitale pourrait être irréversible, car, contrairement au mot de passe qu'on peut réinitialiser à souhait, il est impossible de changer son empreinte digitale qui fait partie intégrante de la personne humaine.

Ainsi dans une interview au Der Spiegel, Johannes Caspar, membre de la CNIL allemande, a mis en garde contre l'utilisation quotidienne des capteurs d'empreinte digitale : « *Les spécificités biométriques de votre corps, telles que vos empreintes digitales, ne peuvent pas être effacées ou supprimées. Elles restent avec vous jusqu'à la fin de vos jours et restent constantes, elles ne peuvent pas être modifiées.* »

Il ressort de ces développements qu'il existe bel et bien des risques que les dispositifs de reconnaissance par empreinte digitale fassent l'objet d'un piratage ou que les données biométriques soient transmises à des tiers, ce qui pourrait entrainer une violation de la vie privée ou une usurpation d'identité.

Mais si ces risques venaient à se réaliser, il y aurait alors toutes les raisons de brandir les

nombreux textes protégeant les données personnelles et la vie privée tels que l'article 9 du code civil, l'article 8 de la Convention européenne des droits de l'homme, ainsi que l'article 226-4-1 du code pénal qui punit l'usurpation d'identité d'un an d'emprisonnement et de 15 000 € d'amende.

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