08 mars 2017

La sécurisation de l'accès à votre smartphone nécessite la mise en place d'une authentification qui peut être un code, un schéma ou, dans certains cas, un dispositif biométrique. Dans ce dernier cas, la CNIL vous informe sur les conditions d'application d'un tel système.

La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Quelques dispositifs d'authentification biométrique :

- **L'authentification par empreinte digitale** : en voie de démocratisation, cette fonctionnalité est proposée par les principaux constructeurs en alternative au code d'accès ou au chemin. L'éditeur doit veiller à ce que le système résiste à des tentatives de piratage classique, notamment, l'utilisation d'une empreinte imprimée à plat.
- **La reconnaissance faciale** : en effectuant un « selfie » grâce à la caméra frontale, votre smartphone reconnait les contours de votre visage et déverrouille l'accès. L'éditeur de la solution biométrique doit s'assurer que le capteur résiste aux attaques telles que l'utilisation d'une photo pour duper la reconnaissance faciale.

Où sont hébergées vos données ?

Il existe deux possibilités :

- **Votre gabarit biométrique est uniquement stocké localement, au sein de l'appareil**. Par exemple, si vous utilisez le système d'authentification de votre smartphone Android ou iPhone, ni les applications, ni le constructeur du téléphone et/ou du système d'exploitation ne peut accéder à votre gabarit. De plus, cette fonctionnalité ne peut être utilisée que pour une seule et même finalité : celle de reconnaitre le possesseur du smartphone. Cette donnée ne peut être extraite de l'appareil ou recoupée avec d'autres.
- **Votre empreinte est enregistrée dans un Cloud, manipulable par des applications voir récupérable par un tiers.** La personne concernée n'a donc pas la maitrise du gabarit biométrique.

Peut-on refuser de recourir à la biométrie ?

Le recours à la biométrie pour accéder à une application doit relever du seul choix de la personne concernée, et ne peut en aucun cas être une obligation. Dans tous les cas, une alternative à la méthode d'authentification non-biométrique doit vous être proposée. Le fournisseur d'une application souhaitant contrôler l'accès de ses utilisateurs par authentification biométrique doit ainsi leur permettre de s'authentifier par un autre moyen - par exemple la saisie d'un code - sans contrainte additionnelle.

Et la sécurité ?

Le fournisseur d'application doit en tout état de cause s'assurer que la solution d'authentification biométrique à laquelle il fait appel (et avec laquelle son application peut échanger) est suffisamment fiable. Les mesures de sécurité sont énumérées dans cette fiche dédiée aux professionnels.

Pour connaitre les autres techniques permettant de sécuriser l'accès à votre smartphone (PIN, verrouillage, chiffrement), rendez-vous sur notre fiche pratique.