Biométrie

https://www.cnil.fr/fr/biometrie

La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.).

Biométrie dans les smartphones

Les mécanismes d'authentification biométriques sur les smartphones se généralisent. La CNIL a établi les conditions dans lesquelles ces traitements de données biométriques sont, ou non, soumis au cadre de protection des données. […]

Deux types de dispositifs :

La reconnaissance biométrique intégrée dans ces appareils peut fonctionner selon deux typologies de configuration, qui n'engendrent pas les mêmes risques pour la vie privée des particuliers, ni le même encadrement juridique :

1. **Les dispositifs biométriques dont le gabarit est stocké dans l'appareil, sous le seul contrôle du particulier.**

De nombreux appareils mobiles intègrent des dispositifs biométriques fonctionnant de manière autonome, dans un environnement totalement cloisonné au sein de l'appareil qui empêche que les données biométriques en elles-mêmes ne soient accessibles à l'extérieur de l'enclave. Dans ces cas, le gabarit biométrique est enregistré dans l'appareil, dans une sorte de « boîte » hermétique, et ne sort jamais de cette « boîte ». En pratique, lorsque l'utilisateur s'authentifie, le doigt posé sur le lecteur de l'appareil est comparé avec le gabarit biométrique préalablement enregistré. Le service ou l'application qui utilise ce mode d'authentification ne reçoit qu'une information sur la réussite ou l'échec de la comparaison entre le doigt présenté et le gabarit. […]

2. **Les dispositifs biométriques fonctionnant depuis des serveurs distants**

Dans d'autres cas, les dispositifs d'authentification basés sur la reconnaissance biométrique fonctionnent en interaction avec des serveurs distants maîtrisés par un organisme tiers, quels qu'ils soient. L'organisme en question (qu'il s'agisse du fournisseur de l'application, de l'appareil, etc.) **doit alors effectuer une analyse d'impact relative à la protection des données (AIPD).** Le traitement de données envisagé est en effet susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées compte-tenu notamment de la sensibilité des données traitées et du caractère innovant des technologies employées. […]