



## La Commission nationale de l'informatique et des libertés

La mise en place d'une solution biométrique suppose une demande d'autorisation préalable à adresser à la CNIL **sauf** télé-déclaration pour les **Autorisations Uniques**.

En biométrie, la CNIL se positionne par rapport à une technologie donnée dans un contexte donné. Exemple : Empreinte Digitale pour le Contrôle d'accès.

A la suite d'une demande d'autorisation préalable, la CNIL statue par **Avis Favorable** ou **Avis Défavorable**.

Il est possible de résumer les positions de la CNIL de la façon suivante :

➤ **Pointage – Gestion de présence :**

Aucune solution biométrique n'est autorisée

➤ **Contrôle d'accès du personnel :**

Quelle que soit la technologie utilisée, la CNIL se positionne en fonction de la méthode de stockage de l'information biométrique :

- Empreinte Digitale
- Morphologie de la Main
- Réseau Veineux
- Reconnaissance faciale :

Pour bénéficier de l'Autorisation Unique AU052, 2 possibilités :

- Le gabarit biométrique doit être stocké dans un badge.
- Le gabarit biométrique peut être stocké dans le lecteur ou en base de données mais crypté avec un code détenu et maîtrisé par le salarié.



L'autorisation unique AU052 est valable pour les dispositifs biométriques mis en œuvre pour contrôler l'accès aux locaux, appareils et applications informatiques utilisés sur les lieux de travail. Ces dispositifs doivent garantir à la personne concernée de garder la maîtrise de son gabarit. Cela suppose de stocker le gabarit biométrique :

- sur un support détenu par la seule personne concernée
- ou en base de données sous une forme inexploitable car illisible sans un code secret détenu par la seule personne concernée.



L'autorisation unique AU053 est valable pour les dispositifs biométrique reposant sur un stockage des gabarits en base (serveur informatique ou lecteur biométrique de lecture comparaison) pour le contrôle d'accès aux locaux, le contrôle d'accès aux appareils ou applications informatiques utilisés sur les lieux de travail.

L'autorisation unique AU053 doit être documentée par l'utilisateur suivant une grille d'analyse à télécharger sur le site de la CNIL.

Pour bénéficier de l'AU053, il est nécessaire que l'application concerne la protection d'un risque justifié.

C'est ainsi qu'a été autorisée la protection par un système d'empreintes digitales avec stockage sur le lecteur-comparaison ou sur un serveur :

- d'une zone spécifique à l'intérieur d'une installation nucléaire de base ;
- de certains sites classés SEVESO II, pour un large périmètre ou seulement pour des zones sensibles, compte tenu de la nature des produits manipulés et de la réglementation applicable en l'espèce (Plan d'Opération Interne imposé par arrêté préfectoral par exemple) ;
- d'une cellule de production des vaccins où se déroulent des cultures bactériennes ;
- d'un bloc opératoire dans un CHU confronté à des problèmes spécifiques d'intrusion liés au voisinage ;
- de l'utilisation d'un matériel dangereux, tels que des chariots élévateurs.

Les accords d'autorisations uniques sont automatiques, il n'y a pas d'autorisation préalable à demander, une simple télé-déclaration en ligne suffit.