Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Préposé fédéral à la protection des données et à la transparence**
**PFPDT**

# Systèmes de vérification et stockage des données

## Contexte

Il est généralement admis que l'emploi multiple de caractères de légitimation présente un risque pour la sécurité, raison pour laquelle il faut l'éviter; nous recommandons dès lors de toute urgence d'utiliser par exemple un code NIP différent pour chaque carte bancaire et de changer ces codes régulièrement. L'utilisation de systèmes de reconnaissance biométriques va dans une direction diamétralement opposée à cette recommandation: d'une part, il n'existe qu'un nombre limité de données biométriques d'épreuve par caractéristique (on n'a par exemple que dix doigts et deux yeux), d'autre part, les systèmes usuels se focalisent sur les mêmes caractéristiques (l'écrasante majorité des systèmes utilise les empreintes digitales). Dans ces conditions, il est impossible d'opérer de grandes variations ou de procéder à des changements réguliers. C'est la raison pour laquelle il faut fixer des exigences particulièrement élevées en ce qui concerne la sécurité entourant le recours aux données biométriques.

Le choix du lieu de stockage des données biométriques revêt une grande importance du point de vue du droit de la protection des données. Le stockage centralisé de ce genre de données entraîne une atteinte assez grande aux droits de la personnalité des personnes concernées. Il est possible d'utiliser les données stockées de cette manière à l'insu des personnes concernées, si bien que ces dernières ne peuvent plus exercer leur droit à l'autodétermination informationnelle dans ce domaine. Le stockage centralisé des données biométriques fait augmenter le risque d'abus étant donné que, d'une part, le volume de ce type de données peut être important, et que, d'autre part, les personnes concernées n'ont aucun contrôle sur les données en question.

On opère une distinction entre deux procédures: l'identification et la vérification. Les **systèmes d'identification** biométriques servent à contrôler l'identité d'une personne présente (à contrôler p. ex. si une personne donnée est bien Madame XY, qui est enregistrée dans la banque de données des collaborateurs). Dans ce cas de figure, on recourt donc à une comparaison 1:n pour contrôler l'identité d'une personne, si bien qu'une banque de données centralisée se révèle nécessaire. La procédure de vérification est différente: si l'on traite les données biométriques dans le but de **vérifier** l'identité prétendue d'une personne (p. ex. pour déterminer si une personne donnée est véritablement le titulaire de l'abonnement qu'elle présente), il n'est pas nécessaire de stocker les données de façon centralisée. Ces procédures de vérification opèrent une comparaison entre une donnée biométrique d'épreuve (p. ex. le doigt appliqué sur le lecteur) et une donnée biométrique de référence (p. ex. l'empreinte digitale de référence enregistrée sur une carte), donc une comparaison 1:1. Voilà pourquoi il faudrait en l'occurrence stocker les données uniquement sur la carte, donc de façon décentralisée, pour respecter le principe de proportionnalité et pour garantir l'autodétermination informationnelle.

Il se peut toutefois que des raisons **rendent une décentralisation impossible** ou alors réalisable uniquement moyennant des frais et des travaux disproportionnés. S'il faut donc mettre en place un système de vérification assorti de données biométriques stockées de façon centralisée, il faut tenir compte d'une autre manière des exigences élevées en termes de protection des données. Les pages suivantes expliquent la manière dont on peut stocker des données biométriques dans le respect de la protection des données en cas de recours à des systèmes de vérification. D'autres solutions – qui ne sont pas présentées ici – sont envisageables dans la mesure où les exigences relevant de la protection des données sont remplies.

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Des informations complémentaires sur le sujet figurent dans notre Guide relatif aux systèmes de reconnaissance biométrique.

## Exigences générales

Les données biométriques brutes contiennent sensiblement plus d'informations sur une personne donnée que les gabarits (voir notre Guide relatif aux systèmes de reconnaissance biométrique), et même, suivant les circonstances, des données sensibles (certaines maladies de l'œil peuvent p. ex. être détectées lors de la numérisation de l'iris). Le recours à des données biométriques brutes constitue ainsi régulièrement une atteinte plus grande aux droits de la personnalité que le recours à des gabarits. En général, l'utilisation de ces derniers dans un système de reconnaissance biométrique suffit. L'atteinte plus grande aux droits de la personnalité que constitue l'utilisation de données brutes est donc inutile et disproportionnée. Il s'agit par conséquent d'utiliser des gabarits à la place des données brutes dans les systèmes de reconnaissance biométriques.

Il convient d'accorder une importance particulière à la sécurité des données en cas de recours à des données biométriques. Ces dernières peuvent être sensibles, sans parler du fait qu'elles peuvent être liées durablement à une personne et difficiles à remplacer en cas d'abus. Aussi faut-il protéger les données biométriques stockées en prenant des mesures supplémentaires (p. ex. chiffrement), quel que soit l'endroit où elles sont stockées.

## Systèmes faisant appel à des supports de données externes

La meilleure façon de préserver l'autodétermination informationnelle consiste à utiliser des systèmes faisant appel à des supports de données externes, comme nous le montrons ci-après.

### Décentralisation

La décentralisation est la meilleure méthode pour garantir l'autodétermination informationnelle de la personne concernée. Voilà pourquoi elle doit être privilégiée. Cette méthode consiste à stocker les données biométriques uniquement sur un support de données externe, par exemple sur une carte à puce, de façon à ce que la personne concernée ait un contrôle exclusif sur ce support de données. La personne en question doit avaliser chaque fois explicitement et consciemment l'utilisation de ses données biométriques, si bien qu'elle sait toujours quand ces dernières sont utilisées. Même si l'on utilise un système sur carte (voir notre Guide relatif aux systèmes de reconnaissance biométrique), les données biométriques ne quittent à aucun moment le giron de la personne concernée, raison pour laquelle cette variante est celle qui garantit le mieux la protection de la personnalité.

Si les données biométriques sont stockées de façon exclusivement décentralisée sur un support de données externe qui est en possession de la personne concernée, et si le droit à l'autodétermination informationnelle est ainsi garanti, il est possible d'utiliser n'importe quelles caractéristiques biométriques pour le système de reconnaissance (caractéristiques avec ou sans traces, voir notre Guide relatif aux systèmes de reconnaissance biométrique).

### «Pseudodécentralisation»

Cette variante fait appel au stockage certes centralisé des données biométriques, mais l'accès à d'autres données personnelles ne peut se faire qu'au moyen d'un code d'attribution distinct pour chaque personne. Ce code est enregistré sur un support de données externe sans que le gestionnaire du système le connaisse. Ce dernier ne peut donc pas dire à qui appartiennent les données biométriques qui sont enregistrées sur son système de façon centralisée. Leur attribution à une personne donnée n'est possible que si la personne en question est là pour utiliser sa carte.

Dès que la carte est lue par le lecteur, la banque de données peut charger le gabarit correspondant et établir la liaison avec les autres données relatives à la personne considérée (p. ex. données d'identité et droits d'accès). L'identité de la personne est vérifiée au moyen de la caractéristique biométrique présentée, après quoi la liaison entre le gabarit et les autres données personnelles est immédiatement interrompue. Il va de soi que les accès aux différents groupes de données ne peuvent pas être répertoriés de telle façon qu'il soit à nouveau possible d'attribuer les données à la personne considérée, par exemple sur la base d'un horodatage concordant.

Par rapport à la décentralisation, cette variante a l'avantage que le fichier enregistré sur le support de données externe (donc le code d'attribution) est d'une taille bien inférieure à celle d'un gabarit, ce qui permet de réduire la capacité de stockage du support externe et d'accroître la rapidité du système.

Etant donné que la pseudodécentralisation fait appel au stockage centralisé des données biométriques, le droit à l'autodétermination informationnelle des personnes concernées s'en trouvé réduit d'autant. Qui plus est, il existe un risque accru que les données soient utilisées abusivement. C'est la raison pour laquelle il faut privilégier les caractéristiques biométriques sans traces dans cette variante (voir notre Guide relatif aux systèmes de reconnaissance biométrique).

## Systèmes ne faisant pas appel à des supports de données externes

### Centralisation

Si l'on souhaite ou si l'on doit renoncer à utiliser des supports de données externes, il faut opter impérativement pour un système de reconnaissance biométrique assorti d'un stockage centralisé. Comme nous l'avons déjà dit précédemment, le stockage centralisé présente un risque d'abus plus élevé lors du traitement des données.

Comme la banque de données centralisée comporte une grande quantité de données biométriques, l'accès à ces données présente un fort attrait, notamment pour des tiers. Aussi faut-il que la sécurité générale des données réponde à des critères très élevés en cas de recours à des systèmes de ce genre. L'exploitant doit pouvoir exclure tout risque que les données puissent être consultées illicitement. Vous trouverez des informations complémentaires sur les mesures de sécurité qui peuvent être prises en la matière dans notre Guide relatif aux mesures techniques et organisationnelles.

Un autre danger réside dans la possibilité d'associer les données. Les données biométriques peuvent être associées à d'autres informations relatives aux personnes concernées ou à d'autres données biométriques, jusqu'à constituer un profil de la personnalité. Dans le domaine de la biométrie, cela peut avoir des conséquences imprévisibles, notamment si différents systèmes d'accès fonctionnent avec la même empreinte digitale, car on pourrait déterminer quand une personne donnée était dans

un club de sport puis dans une discothèque, et dresser ainsi le profil de ses déplacements. Plus une empreinte digitale est utilisée souvent, plus la situation sera grave en cas de perte de la donnée biométrique de base correspondante. Voilà pourquoi il faut stocker les données biométriques de telle manière qu'on ne puisse pas établir de lien avec d'autres données personnelles. En d'autres termes, les données doivent être sauvegardées dans une mémoire distincte, où ne sont stockées ni les données d'identité des personnes concernées ni leurs pseudonymes (p. ex. les numéros de collaborateur). La personne qui traite les données ne doit pas pouvoir établir de lien entre les données disponibles, ni par le biais d'une liste d'attribution ni par celui de l'horodatage ou par un moyen de ce genre. Par ailleurs, le support de données ne doit être équipé d'aucun moyen permettant de communiquer avec d'autres appareils, si bien qu'il serait possible d'utiliser par exemple un système autonome (*standalone*) de contrôle des accès qui ne soit équipé d'aucun dispositif de raccordement permettant de lire les données biométriques qu'il contient.

Le stockage centralisé des données biométriques entraîne une restriction accrue du droit à l'autodétermination informationnelle. Le risque d'abus est encore plus élevé que dans le cas de la «pseudodécentralisation» décrite plus haut étant donné que l'utilisation de ce genre de systèmes ne nécessite pas de support de données externe, mais aussi que le contrôle du droit d'accès repose uniquement sur la caractéristique biométrique. En étant en possession des données biométriques concernant une personne donnée, il est aisé de se faire passer pour elle face au système – ce qui constituerait une usurpation d'identité –, car il n'est pas nécessaire d'effectuer une légitimation supplémentaire au moyen d'un jeton (*token*). C'est la raison pour laquelle il faut utiliser exclusivement des caractéristiques biométriques qui ne laissent pas de traces avec les systèmes d'accès biométriques fonctionnant avec une banque de données centralisée. Ces caractéristiques, notamment le réseau veineux de la main ou du doigt, ne laissent pas de traces et ne peuvent pas être lues de l'extérieur, contrairement aux caractéristiques qui laissent des traces, comme les empreintes digitales (voir notre Guide relatif aux systèmes de reconnaissance biométrique [lien]). On peut dès lors en exclure que ces caractéristiques peuvent être collectées à l'insu de la personne concernée.

| **Décentralisation** | **Pseudodécentralisation** | **Centralisation** |
|---|---|---|
| Caractéristiques biométriques **avec ou sans traces**<br><br>Données biométriques stockées **de façon décentralisée** sur des cartes à puce | Caractéristiques biométriques **avec ou sans traces**<br><br>Données biométriques stockées **de façon centralisée**<br><br>**Lien** avec d'autres données personnelles pouvant être établi uniquement au moyen d'une **carte** | Uniquement caractéristiques biométriques **sans traces**<br><br>Données biométriques stockées **de façon centralisée**<br><br>**Aucun lien** avec d'autres données personnelles |

Etat : juillet 2013