Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol

FAQ – AFIS2026

Quelle est la différence entre la reconnaissance faciale (*face recognition*) et la comparaison d'images faciales (*facial comparison*)?

- La différence entre la reconnaissance faciale et la comparaison d'images faciales réside dans l'application de la technologie.
- La reconnaissance faciale désigne la supra-catégorie, qui comprend notamment les sous-catégories suivantes:
  - la surveillance en temps réel ou *live scan* (n'est pas appliquée)
  - la comparaison d'images faciales (est appliquée avec AFIS2026)

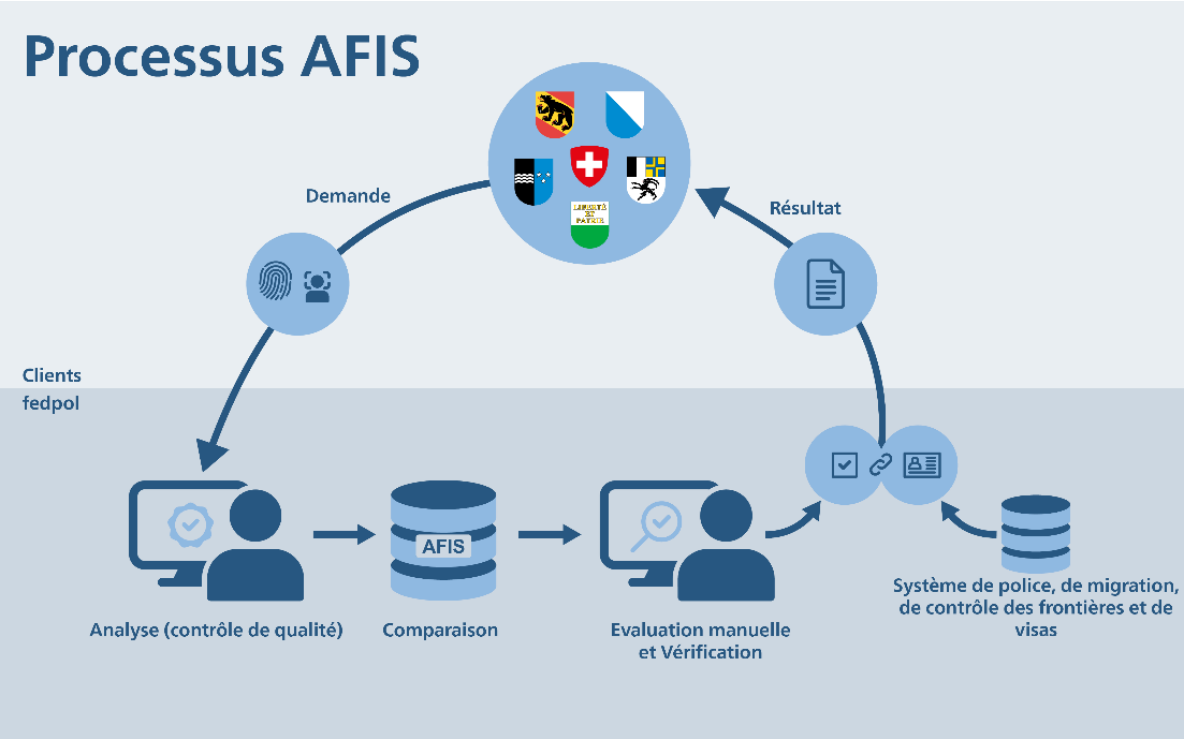
Pourquoi ne pas utiliser le *live scan*?
Dans le cadre du projet AFIS2026, la reconnaissance faciale en temps réel (live scan) au moyen de caméras, n'est pas utilisée car il n'existe pas de base légale qui le permet. Il n'est pas non plus prévu de créer une telle base légale pour AFIS.

Qu'est-ce que la "comparaison d'images faciales"?
Le système fonctionne de la même manière que pour la comparaison des empreintes digitales: il permet par exemple, dans le cadre d'une procédure pénale, de comparer une image d'un suspect avec des images signalétiques enregistrées dans le système AFIS. Les méthodes de reconnaissance d'aujourd'hui font appel à des algorithmes perfectionnés et ultra-modernes. Ces derniers filtrent parmi les images faciales enregistrées celles qui peuvent entrer en considération sur la base des caractéristiques biométriques (des visages) et du degré de concordance. En cas de concordance possible (proposée par le système), un spécialiste procède à une vérification manuelle afin de rendre le résultat encore plus fiable.

Qui utilise cette technologie en Europe?
Dans l'UE, la comparaison d'images faciales fait désormais partie intégrante du traitement des données biométriques, en plus des empreintes digitales et de l'ADN. Plusieurs pays européens – dont l'Allemagne, la Grande-Bretagne et les Pays-Bas – ont une longue expérience de la comparaison d'images faciales. Comme on a par exemple pu l'observer en Allemagne, des affaires restées non résolues en raison de l'absence de traces ont pu être élucidées grâce à la comparaison d'images faciales, laquelle constitue un outil supplémentaire de soutien aux enquêtes. La possibilité de pouvoir comparer des données supplémentaires contribue à augmenter le taux d'élucidation des infractions et de l'identification de personnes.

Comment fonctionne la comparaison d'images faciales concrètement?

- L'image faciale arrive dans le système et est soumise à un contrôle de qualité.
- Le système analyse l'image et en extrait des points caractéristiques.
- Avec ces points, le système crée un modèle, une structure (en anglais: *template*).
- Ce modèle est comparé avec ceux enregistrés dans la banque de données.
- Le système propose une liste de candidats en fonction d'un taux de probabilité (liste de *matchs* potentiels).
- Ces propositions sont vérifiées par des experts.



Sur quelles bases légales est-il possible de faire une comparaison d'images faciales en Suisse?
L'art. 354 du Code pénal (CP; RS 311.0) constitue la base légale pour le système d'information AFIS, notamment en ce qui concerne l'enregistrement, le stockage et la comparaison de données signalétiques biométriques. En vertu de l'art. 354, al. 1, CP en relation avec l'art. 2, let. c, de l'ordonnance du 6 décembre 2013 sur le traitement des données signalétiques biométriques (RS 361.3), il est possible de comparer entre eux des données et des traces dactyloscopiques (par ex. empreintes digitales), des signalements (descriptions de personnes), et notamment aussi des photographies. Cette comparaison ne peut être effectuée qu'aux fins d'identifier une personne recherchée ou inconnue ou des traces relevées sur les lieux d'une infraction. Conformément à l'art. 14, al. 2, de la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP; RS 361), fedpol peut également traiter des photographies dans le système AFIS. Cette possibilité n'a pas encore été exploitée pour le moment pour des raisons techniques et financières.

Le Préposé fédéral à la protection des données a-t-il approuvé le projet?
Afin de respecter les exigences élevées de notre État de droit, les différents cas d'application (comparaison d'images faciales des catégories personne-personne, personne-trace, trace-trace et trace-personne) ont fait l'objet d'un nouvel examen critique quant à leur conformité légale, également au regard des prescriptions de la nouvelle loi sur la protection des données. Le Préposé fédéral à la protection des données a approuvé le projet AFIS2026.

Pourquoi doit-on renouveler AFIS?
Le système AFIS actuel introduit en 2016 est conçu pour une durée de fonctionnement de dix ans. Il arrivera donc en fin de vie en 2026, tant du point de vue technique que contractuel. Le projet AFIS2026 vise à remplacer le système actuel par un nouveau système d'ici à 2026 qui aura l'avantage de bénéficier des avancées technologiques significatives réalisées dans le domaine des méthodes d'identification d'empreintes digitales et palmaires.

Quelles seraient les conséquences si AFIS2026 n'était pas concrétisé?
Le renouvellement du système AFIS est nécessaire pour différents projets et développements en cours. Il s'agit notamment du SIS (Système d'information Schengen), de Next Generation Prüm et de l'EES (Entry/Exit System). L'abandon du projet AFIS2026 pourrait ralentir ou retarder certains projets majeurs nécessaires à une bonne coopération policière.
De plus, la lutte contre la criminalité et notamment la résolution d'affaires criminelles seraient moins efficaces si cette technologie n'était pas utilisée.

Quand AFIS2026 pourra entrer en fonction?
L'introduction du nouveau système comprenant le module de comparaison d'images faciales est prévue pour la fin de 2026. Le projet AFIS2026 ajoute un chapitre à la belle histoire d'AFIS qui a commencé il y a presque 40 ans, en rendant possible la comparaison d'images faciales. Il s'agit de continuer à développer et à mettre à niveau l'identification biométrique de personnes et de traces pour lutter contre la criminalité, en se fondant sur les bases légales déjà en vigueur.

Est-ce que la comparaison d'images faciales est sûre?
Le système fonctionne de la même façon que pour la comparaison des empreintes digitales: il permet par exemple, dans le cadre d'une procédure pénale, de comparer une image d'un suspect avec les images signalétiques enregistrées dans le système AFIS. Les méthodes de reconnaissance d'aujourd'hui font appel à des algorithmes perfectionnés et ultramodernes. Ces derniers filtrent parmi les images faciales enregistrées celles qui peuvent entrer en considération sur la base des caractéristiques biométriques (des visages) et du degré de concordance. En cas de concordance possible (proposée par le système), un spécialiste procède à une vérification manuelle afin de rendre le résultat encore plus fiable.

Des personnes peuvent-elles être accusées à tort?
La comparaison d'images faciales est un outil de soutien aux enquêtes, pas une preuve en soi. Comme pour les empreintes digitales, les résultats sont toujours vérifiés par des experts. Ce n'est jamais le système qui décide.

Pour quels types de délits pourra-t-on utiliser la comparaison d'images faciales?
L'utilisation de la comparaison d'images faciales, tout comme l'utilisation d'empreintes digitales, est strictement réglée par le droit suisse. Conformément à l'art. 354, al. 1, CP s'agissant des traces, et en vertu de l'art. 260 du code de procédure pénale (CPP; RS 312.0), la police, le ministère public et les tribunaux peuvent ordonner la saisie des données signalétiques d'une personne, par exemple en cas de viol, d'assassinat, de vol avec effraction ou d'enlèvement.

Est-il possible de tromper cette technologie (par ex. par du *morphing*)?
Les images de personnes enregistrées dans la banque de données sont prises par les autorités (par ex. photos d'identification ou vues de face et de profil).
Les images de traces sont analysées et présentées en premier lieu par le service de police scientifique. Les tentatives de *morphing* sont souvent reconnaissables dans les métadonnées des images et connues des services de police scientifique. Par ailleurs, les images publiques, par exemple tirées d'Instagram ou de Facebook, ne sont jamais utilisées dans AFIS, ce qui minimise le risque de *morphing*. De plus, l'image n'est toujours qu'un indice d'enquête, jamais une identification définitive.
Exemple: lorsqu'un témoin filme un acte avec son téléphone portable ou qu'une caméra de surveillance privée a été utilisée, le service de police scientifique doit toujours contrôler les images pour voir s'il y a eu des tentatives de morphing. Cela fait partie du contrôle de qualité manuel des images (traces faciales) avant qu'elles ne soient enregistrées dans le système.