Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Polizei fedpol
Kommunikation

FAQ – AFIS2026

Qual è la differenza tra il riconoscimento facciale («face recognition») e il confronto di immagini del volto («facial comparison»)?

- La differenza tra il riconoscimento facciale e il confronto delle immagini del volto consiste nell'applicazione della tecnologia.
- Il riconoscimento facciale definisce la categoria superiore, mentre le sottocategorie sono:
  - la sorveglianza in tempo reale o «live scan» (sottocategoria non applicata);
  - il confronto delle immagini del volto (sottocategoria applicata nell'ambito di AFIS2026)

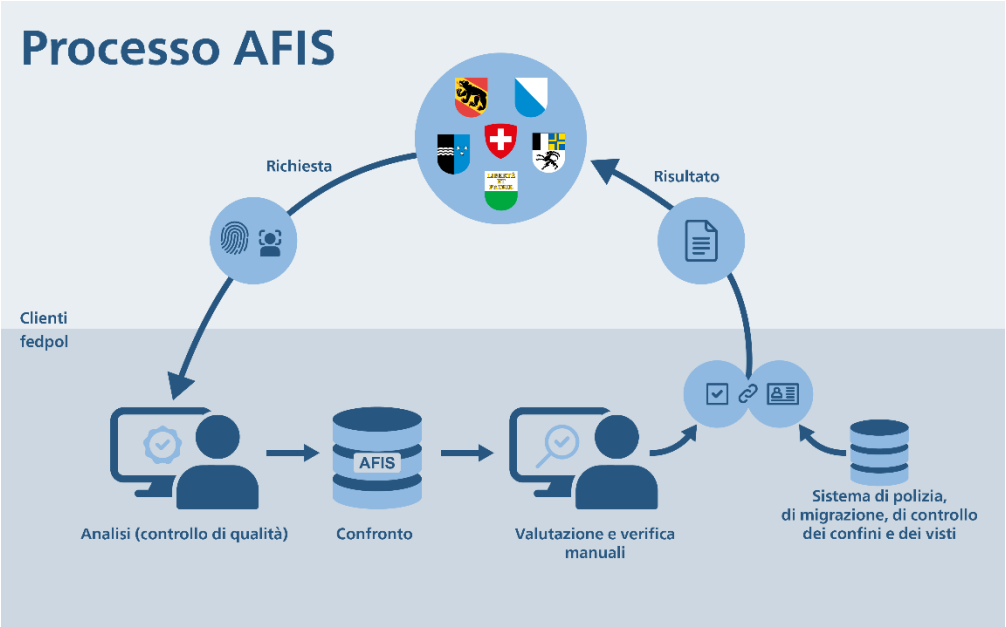
Perché non utilizzare il «live scan»?
Nel contesto del progetto AFIS2026, il riconoscimento facciale in tempo reale basato su telecamere («live scan») non viene utilizzato poiché non esiste alcuna base legale per farlo. Non è prevista neanche la creazione di una base legale del genere per AFIS.

Cosa s'intende per confronto delle immagini del volto?
Il confronto delle immagini del volto funziona allo stesso modo del confronto delle impronte digitali: consente, per esempio, nell'ambito di un procedimento penale di confrontare un'immagine di una persona sospetta con le immagini segnaletiche già registrate nel sistema AFIS. Le procedure di riconoscimento utilizzate attualmente fanno capo ad algoritmi perfezionati e sofisticati. Questi algoritmi si servono delle caratteristiche biometriche (dei volti) per proporre, in funzione del grado di corrispondenza, una selezione delle immagini del volto registrate nel sistema. In caso di possibile corrispondenza proposta dal sistema, un esperto effettuerà una verifica manuale rendendo quindi il risultato ancora più attendibile.

In Europa, quali Paesi utilizzano questa tecnologia?
Nell'UE il confronto delle immagini del volto diventa parte integrante del trattamento dei dati biometrici, insieme alle impronte digitali e al DNA. Diversi Paesi europei, tra cui la Germania, la Gran Bretagna e i Paesi Bassi, hanno maturato un'esperienza pluriennale in materia di confronto delle immagini del volto. In Germania, per esempio, è stato osservato che il confronto delle immagini del volto, quale strumento supplementare di sostegno alle indagini, consente di far luce su casi che, in precedenza, non era stato possibile risolvere per mancanza di tracce. Il confronto di un dato aggiuntivo incide quindi positivamente sul tasso di chiarimento dei reati e di identificazione delle persone.

In concreto, come funziona il confronto delle immagini del volto?

- L'immagine del volto arriva nel sistema ed è sottoposta a un controllo di qualità.
- Il sistema analizza l'immagine e ne estrae i punti caratteristici.
- Il sistema utilizza questi punti per creare un modello, una struttura (in inglese «template»).
- Questo modello è confrontato con quelli già registrati nella banca dati.
- Il sistema propone un elenco di candidati in base a un valore di verosimiglianza (elenco di possibili corrispondenze).
- Queste proposte sono verificate da esperti.



Quali basi giuridiche permettono di eseguire il confronto delle immagini del volto in Svizzera?
L'articolo 354 del Codice penale (CP; RS *311.0*) costituisce la base legale per il sistema d'informazione AFIS, in particolare per quanto concerne la registrazione, il salvataggio e il confronto di dati biometrici ai fini dell'identificazione. Secondo l'articolo 354 capoverso 1 CP in combinato disposto con l'articolo 2 lettera c dell'ordinanza del 6 dicembre 2013 sul trattamento dei dati segnaletici di natura biometrica (RS *361.3*), possono essere confrontati i dati dattiloscopici e le tracce (p. es. le impronte digitali), i connotati (descrizioni di persone) e in particolare le fotografie. Tale confronto può essere eseguito unicamente allo scopo di identificare una persona ricercata o sconosciuta e per l'identificazione di tracce rinvenute sul luogo di un reato. fedpol può trattare fotografie in AFIS in virtù dell'articolo 14 capoverso 2 della legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione (LSIP; RS *361*). Finora questa possibilità non è stata ancora sfruttata per motivi meramente tecnici e finanziari.

Il progetto è stato approvato dall'Incaricato federale della protezione dei dati e della trasparenza?
Al fine di rispettare le esigenze elevate del nostro Stato di diritto, i diversi casi di applicazione (confronto delle immagini del volto delle categorie persona-persona, persona-traccia, traccia-traccia e traccia-persona) sono stati sottoposti nuovamente a un esame critico in merito alla loro conformità con la legge, naturalmente anche alla luce delle disposizioni della nuova legge federale del 25 settembre 2020 sulla protezione dei dati (LPD; RS *235.1*). Il progetto AFIS2026 ha ottenuto l'approvazione dell'Incaricato federale della protezione dei dati e della trasparenza.

Perché occorre rinnovare AFIS?
L'attuale sistema AFIS è stato introdotto nel 2016 ed è stato concepito per una durata di funzionamento di dieci anni. Nel 2026 raggiungerà pertanto la fine del suo ciclo di vita da un punto di vista sia tecnico sia contrattuale. Il progetto AFIS2026 si prefigge di sostituire il sistema attuale con il nuovo sistema entro il 2026. Intende inoltre trarre beneficio dai considerevoli progressi tecnologici realizzati nei metodi di identificazione delle impronte digitali e palmari.

Quali sarebbero le ripercussioni se AFIS2026 non venisse realizzato?
Il rinnovo del sistema AFIS è necessario nell'ambito di diversi progetti e sviluppi in corso, più

precisamente di SIS (Sistema d'informazione Schengen), Next Generation Prüm ed EES (sistema di ingressi/uscite). L'abbandono del progetto AFIS2026 potrebbe rallentare o ritardare diversi progetti di ampia portata necessari a una buona cooperazione di polizia.
Il fatto di non utilizzare la tecnologia offerta dal nuovo sistema costituirebbe inoltre un notevole svantaggio nella lotta contro la criminalità in generale e nel chiarimento di reati in particolare.

Quando potrebbe entrare in funzione AFIS2026?
L'introduzione del nuovo sistema comprendente il confronto delle immagini del volto è prevista per la fine del 2026. Il progetto AFIS2026 porta avanti la storia di successo di AFIS, iniziata quasi 40 anni fa, completandola con il confronto delle immagini del volto. Si tratta di uno sviluppo moderno dell'identificazione biometrica di persone e tracce per una lotta contro la criminalità fondata su basi giuridiche già esistenti.

Il confronto delle immagini del volto è una tecnologia sicura?
Il confronto delle immagini del volto funziona allo stesso modo del confronto delle impronte digitali: consente, per esempio, nell'ambito di un procedimento penale di confrontare un'immagine di una persona sospetta con le immagini segnaletiche già registrate nel sistema AFIS. Le procedure di riconoscimento utilizzate attualmente fanno capo ad algoritmi perfezionati e sofisticati. Questi algoritmi si servono delle caratteristiche biometriche (dei volti) per proporre, in funzione del grado di corrispondenza, una selezione delle immagini del volto registrate nel sistema. In caso di possibile corrispondenza proposta dal sistema, un esperto effettuerà una verifica manuale rendendo quindi il risultato ancora più attendibile.

È possibile che persone vengano accusate ingiustamente?
Il confronto delle immagini del volto è uno strumento di sostegno alle indagini, non costituisce una prova. Come nel caso delle impronte digitali, i risultati sono sempre verificati da esperti. Il sistema stesso non prende mai alcuna decisione.

Per quale tipo di reato sarà possibile utilizzare il confronto delle immagini del volto?
Il ricorso al confronto delle immagini del volto è disciplinato in modo rigoroso dal diritto svizzero, così come lo è l'utilizzo delle impronte digitali. Conformemente all'articolo 354 capoverso 1 del Codice penale (CP; RS *311.0*), per quanto riguarda le tracce, e all'articolo 260 del Codice di procedura penale (CPP; RS *312.0*) la polizia, il pubblico ministero e il giudice possono disporre il rilevamento segnaletico per esempio in caso di violenza carnale, di omicidio, di furto con scasso o di rapimento.

È possibile trarre in inganno questa tecnologia (p. es. tramite «morphing»)?
Le immagini delle persone registrate nella banca dati sono state scattate dalle autorità (p. es. foto segnaletiche come le immagini di identificazione o le fotografie di fronte e di profilo).
Le immagini di tracce sono analizzate e trasmesse in primo luogo dalla polizia scientifica. I tentativi di «morphing» possono essere spesso svelati tramite i metadati delle immagini e sono una pratica nota ai servizi di polizia scientifica. Il rischio di «morphing» è ridotto dal fatto che in AFIS non sono utilizzate immagini pubbliche tratte, per esempio, da Instagram o Facebook. L'immagine costituisce sempre e soltanto un indizio per le indagini, mai un'identificazione chiara.
Esempio: quando un atto è ripreso da un testimone con il telefono cellulare o da una videocamera di sorveglianza privata, la polizia scientifica deve verificare le immagini per accertare eventuali tentativi di «morphing». Questa procedura rientra nel controllo di qualità manuale delle immagini (tracce facciali) effettuato prima che le immagini siano registrate nel sistema.