Come utilizzo il riconoscimento facciale per trovare le persone

Maria Cattini | 08/09/2025 | Open source intelligence

Se ti dicessero che una semplice foto può aprire le porte dell'identità digitale di una persona, ci crederesti? Nell'era dei social network, delle foto profilo e delle piattaforme pubbliche, il volto è diventato una chiave d'accesso alle informazioni. Non si tratta di magia, ma di **riconoscimento facciale applicato all'OSINT (Open Source Intelligence)**.

Questa tecnica è oggi usata da giornalisti investigativi, ricercatori e anche da curiosi che vogliono capire di più su chi hanno davanti. Ma come funziona davvero e quali sono i limiti etici e pratici?

Reverse Image Search: il primo passo

Il punto di partenza è la **ricerca inversa delle immagini**.
Non sempre serve un software avanzato: a volte basta caricare la foto su **Google Images** o su **Yandex**, che hanno algoritmi capaci di individuare immagini identiche o simili pubblicate sul web.

Esempio pratico:

• Carico una foto su Google Images.
• Ottengo come risultato un profilo LinkedIn, un post di Facebook e persino un articolo locale che contiene lo stesso volto.

Il limite? Questi motori riconoscono bene immagini identiche, meno le variazioni (filtri, tagli, qualità bassa).

Il passo successivo: i motori di riconoscimento facciale

Quando la ricerca inversa non basta, entrano in gioco piattaforme specializzate.

PimEyes

È uno dei servizi più noti.

• Come funziona: carichi una foto del volto e il sistema la confronta con miliardi di immagini sul web.
• Risultato: una galleria di volti simili, con link diretti alle pagine in cui appaiono.
• Limite: è a pagamento, ma permette di scaricare le immagini trovate e rilanciarle su Google per un ulteriore incrocio.

FaceCheck ID

Molto simile a PimEyes, con una particolarità: assegna un punteggio di accuratezza (da 50 a 100). Più alto è il numero, più il match è attendibile.

• Un volto con punteggio 90, ad esempio, ha una probabilità molto alta di essere lo stesso individuo.

Tecnica combinata: scaricare, rilanciare, verificare

Gli analisti OSINT raramente si fermano al primo risultato. Una buona prassi è:

1. Usare PimEyes o FaceCheck per ottenere foto correlate.
2. Scaricare ogni immagine trovata.
3. Rilanciarle su Google, Bing o Yandex.
4. Verificare se da lì emergono profili social, forum o articoli che collegano il volto a un nome.

Questo approccio a “catena” aumenta la probabilità di identificare correttamente una persona senza affidarsi ciecamente a un unico tool.

Esempi concreti di utilizzo

• Indagini giornalistiche: un reporter che vuole identificare una fonte anonima può partire da una foto pubblicata su Telegram e rintracciare collegamenti con un profilo pubblico.
• Ricerche familiari: persone adottate o in cerca di parenti usano questi strumenti per rintracciare somiglianze in foto vecchie e archivi digitali.
• Verifica identità online: sempre più utenti controllano chi c’è dietro un profilo sospetto prima di interagire.

Rischi e limiti etici

Nonostante l’efficacia, il riconoscimento facciale apre questioni delicate:

• Privacy: caricare una foto altrui senza consenso può violare diritti personali.
• Falsi positivi: non sempre il volto corrisponde esattamente, con il rischio di attribuire identità sbagliate.
• Abusi: da parte di stalker, truffatori o regimi repressivi.

Per questo motivo, gli esperti OSINT consigliano sempre di **contestualizzare e incrociare i dati**. Una foto da sola non basta: serve riscontro da più fonti indipendenti.

Tutorial rapido: trovare una persona da una foto

1. Carica l’immagine su Google Images per verificare copie identiche.
2. Prova con Yandex, più forte sul riconoscimento facciale rispetto a Google.
3. Passa a PimEyes o FaceCheck ID per individuare varianti e somiglianze.
4. Scarica ogni match rilevante e rilancialo nei motori di ricerca.
5. Incrocia i dati con altri strumenti OSINT (nome utente, email, domini).

Pro e contro degli strumenti di riconoscimento facciale

Pro

• Rapidi e precisi nel rintracciare immagini pubbliche.
• Utile per giornalismo investigativo, sicurezza e ricerca di persone scomparse.
• Accessibili anche a utenti non tecnici.

Contro

• Costi elevati per le versioni premium.
• Rischio di violazione della privacy.
• Possibili errori di attribuzione.

Il riconoscimento facciale in ambito OSINT è una lama a doppio taglio. Da un lato, offre strumenti potenti per ricostruire identità e connessioni online. Dall'altro, espone al pericolo di violazioni della privacy e abusi.

La regola d'oro? **Usare sempre questi strumenti con senso critico e responsabilità**. Non basta trovare una foto: serve verificare, contestualizzare, e rispettare i limiti etici.

La prossima volta che carichi una tua foto online, pensa a questo: potrebbe essere il punto di partenza per chiunque voglia sapere di più su di te.
Se ti dicessero che una semplice foto può aprire le porte dell'identità digitale di una persona, ci crederesti? Nell'era dei social network, delle foto profilo e delle piattaforme pubbliche, il volto è diventato una chiave d'accesso alle informazioni. Non si tratta di magia, ma di **riconoscimento facciale applicato all'OSINT (Open Source Intelligence)**.

Questa tecnica è oggi usata da giornalisti investigativi, ricercatori e anche da curiosi che vogliono capire di più su chi hanno davanti. Ma come funziona davvero e quali sono i limiti etici e pratici?

Reverse Image Search: il primo passo

Il punto di partenza è la **ricerca inversa delle immagini**.
Non sempre serve un software avanzato: a volte basta caricare la foto su **Google Images** o su **Yandex**, che hanno algoritmi capaci di individuare immagini identiche o simili pubblicate sul web.

Esempio pratico:

• Carico una foto su Google Images.
• Ottengo come risultato un profilo LinkedIn, un post di Facebook e persino un articolo locale che contiene lo stesso volto.

Il limite? Questi motori riconoscono bene immagini identiche, meno le variazioni (filtri, tagli, qualità bassa).

Il passo successivo: i motori di riconoscimento facciale

Quando la ricerca inversa non basta, entrano in gioco piattaforme specializzate.

PimEyes

È uno dei servizi più noti.

• Come funziona: carichi una foto del volto e il sistema la confronta con miliardi di immagini sul web.
• Risultato: una galleria di volti simili, con link diretti alle pagine in cui appaiono.
• Limite: è a pagamento, ma permette di scaricare le immagini trovate e rilanciarle su Google per un ulteriore incrocio.

FaceCheck ID

Molto simile a PimEyes, con una particolarità: assegna un punteggio di accuratezza (da 50 a 100). Più alto è il numero, più il match è attendibile.

• Un volto con punteggio 90, ad esempio, ha una probabilità molto alta di essere lo stesso individuo.

Tecnica combinata: scaricare, rilanciare, verificare

Gli analisti OSINT raramente si fermano al primo risultato. Una buona prassi è:

1. Usare PimEyes o FaceCheck per ottenere foto correlate.
2. Scaricare ogni immagine trovata.
3. Rilanciarle su Google, Bing o Yandex.
4. Verificare se da lì emergono profili social, forum o articoli che collegano il volto a un nome.

Questo approccio a “catena” aumenta la probabilità di identificare correttamente una persona senza affidarsi ciecamente a un unico tool.

Esempi concreti di utilizzo

• Indagini giornalistiche: un reporter che vuole identificare una fonte anonima può partire da una foto pubblicata su Telegram e rintracciare collegamenti con un profilo pubblico.
• Ricerche familiari: persone adottate o in cerca di parenti usano questi strumenti per rintracciare somiglianze in foto vecchie e archivi digitali.
• Verifica identità online: sempre più utenti controllano chi c’è dietro un profilo sospetto prima di interagire.

Rischi e limiti etici

Nonostante l’efficacia, il riconoscimento facciale apre questioni delicate:

• Privacy: caricare una foto altrui senza consenso può violare diritti personali.
• Falsi positivi: non sempre il volto corrisponde esattamente, con il rischio di attribuire identità sbagliate.
• Abusi: da parte di stalker, truffatori o regimi repressivi.

Per questo motivo, gli esperti OSINT consigliano sempre di **contestualizzare e incrociare i dati**. Una foto da sola non basta: serve riscontro da più fonti indipendenti.

Tutorial rapido: trovare una persona da una foto

1. Carica l’immagine su Google Images per verificare copie identiche.
2. Prova con Yandex, più forte sul riconoscimento facciale rispetto a Google.
3. Passa a PimEyes o FaceCheck ID per individuare varianti e somiglianze.
4. Scarica ogni match rilevante e rilancialo nei motori di ricerca.
5. Incrocia i dati con altri strumenti OSINT (nome utente, email, domini).

Pro e contro degli strumenti di riconoscimento facciale

Pro

• Rapidi e precisi nel rintracciare immagini pubbliche.
• Utile per giornalismo investigativo, sicurezza e ricerca di persone scomparse.
• Accessibili anche a utenti non tecnici.

Contro

• Costi elevati per le versioni premium.

• Rischio di violazione della privacy.
• Possibili errori di attribuzione.

Il riconoscimento facciale in ambito OSINT è una lama a doppio taglio. Da un lato, offre strumenti potenti per ricostruire identità e connessioni online. Dall’altro, espone al pericolo di violazioni della privacy e abusi.

La regola d’oro? **Usare sempre questi strumenti con senso critico e responsabilità**. Non basta trovare una foto: serve verificare, contestualizzare, e rispettare i limiti etici.

La prossima volta che carichi una tua foto online, pensa a questo: potrebbe essere il punto di partenza per chiunque voglia sapere di più su di te.