

Perché Google Lens ha scambiato un ex investigatore per un ricercato

Maria Cattini | 14/08/2026 | Sicurezza digitale

Durante un webinar dedicato alle tecniche di investigazione OSINT, Mark Bentley — quasi quarant'anni come detective tra National Crime Agency, Metropolitan Police e Child Exploitation and Online Protection Command — ha caricato su Google Lens una propria foto scattata davanti a un'ambasciata. Il sistema ha restituito una corrispondenza: il suo volto associato al profilo di una persona ricercata. Non era lui. Era un errore del riconoscimento facciale, quella che in gergo si chiama allucinazione algoritmica: il sistema non ammette di non sapere, produce comunque una risposta plausibile.

Se capita a un professionista che sta dimostrando apposta i limiti dello strumento, immagina cosa può succedere a chi usa lo stesso strumento per farsi un'idea su uno sconosciuto — un venditore online, un profilo che chiede l'amicizia, un candidato al colloquio, un contatto di lavoro mai incontrato di persona. Un singolo risultato di ricerca per immagini, preso per buono, può trasformare un'identità sbagliata in un sospetto reale nella tua testa. Ed è esattamente il problema che la metodologia OSINT prova a risolvere: non trovare informazioni, ma [non fidarsi di una sola fonte](#) prima di trovarle davvero.

Cos'è, in pratica, un'indagine OSINT

OSINT sta per Open Source Intelligence: raccolta e analisi di informazioni disponibili pubblicamente — profili social, numeri di telefono, indirizzi email, immagini, dati di violazioni note. Non richiede accesso a sistemi privati né competenze da hacker. Richiede metodo.

Bentley riassume l'approccio in tre fasi, che vale la pena tenere a mente anche fuori dal contesto investigativo professionale, ogni volta che si prova a verificare chi c'è dall'altra parte di uno schermo.

La prima fase è il punto di partenza, il **pivot**: un solo dato iniziale, che sia un'email, un numero di telefono, un nome utente o un'immagine. Da lì si parte, non si arriva. La seconda fase è la **verifica**: nessun dato trovato online va considerato vero finché non trova un riscontro incrociato, indipendente dalla prima fonte. La terza è la **valutazione**: solo dopo aver raccolto più elementi corroborati si può costruire un quadro complessivo, e anche in quel momento resta un quadro probabile, non una certezza assoluta.

Il punto debole di questo processo, quando viene saltato, è sempre lo stesso: fermarsi al primo risultato.

Il metodo, passo per passo

Primo passo: definisci il dato di partenza e isolalo. Se hai un'email sospetta, un profilo social o un numero di telefono, prendi solo quello. Non partire già con un'ipotesi su chi sia la persona: l'ipotesi arriva dopo, dai dati, non prima.

Secondo passo: proteggi il dispositivo prima di cercare, non dopo. Ogni ricerca lascia tracce

— pixel di tracciamento nascosti nelle pagine, crawler che registrano la visita, notifiche che avvertono l'account cercato che qualcuno lo sta osservando. Prima di aprire profili o siti sospetti, usa un browser con protezioni attive (opzioni "Do Not Track", blocco tracker) o una macchina virtuale se l'indagine è delicata. Nessuna di queste misure è infallibile, ma riduce il rischio di essere notati o tracciati a propria volta. Un controllo utile e gratuito: il sito tosdr.org riassume in modo leggibile cosa i termini di servizio di un'app o piattaforma dicono davvero sulla raccolta dati, evitando di doverli leggere per intero.

Terzo passo: interroga più fonti sullo stesso dato, non una sola. Un'email può essere verificata su più strumenti che controllano se compare in violazioni di dati note — [Have I Been Pwned](#) è il più conosciuto e gratuito — o se è collegata ad account su servizi specifici. Un numero di telefono può essere controllato per operatore e formato, poi incrociato con directory pubbliche per vedere se emergono nomi associati. Un'immagine va passata per una ricerca inversa (per esempio TinEye) e, se possibile, analizzata nei metadati con uno strumento come ExifTool, che può rivelare data, dispositivo o posizione di scatto — quando questi dati non sono stati rimossi.

Quarto passo: applica la regola ABC prima di considerare un dato affidabile. Acquisisci il dato, conservane una copia (screenshot, salvataggio della pagina, non solo il link, che può sparire), e cercane conferma indipendente. Se una sola fonte dice una cosa e nessun'altra la conferma, quel dato resta un'ipotesi, non un fatto.

Quinto passo: aggrega solo dopo aver verificato, non prima. Esistono piattaforme che interrogano centinaia di database contemporaneamente per velocizzare la ricerca — durante il webinar è stata usata UserSearch come esempio, con una funzione basata su modelli linguistici (Sargebot) per incrociare frammenti di email, numero e foto in un report automatico. Questo tipo di strumento accelera la raccolta, non sostituisce la verifica: un aggregatore che restituisce dieci corrispondenze ha comunque bisogno che tu ne controlli l'attendibilità una per una, esattamente come per la singola ricerca su Google Lens dell'esempio iniziale.

Gli errori più comuni

Il primo errore è trattare un singolo risultato come una prova. È quello che è successo con Google Lens: un'associazione visiva sbagliata, presa per buona, avrebbe potuto costruire un sospetto infondato su una persona reale.

Il secondo è cercare senza pensare a chi vede la ricerca. Molti strumenti — anche quelli "innocui" come una verifica email — notificano al servizio che qualcuno ha effettuato quel controllo, o lasciano tracce che permettono di risalire a chi ha cercato. Chi indaga senza precauzioni rischia di avvisare proprio la persona che sta osservando.

Il terzo è confondere velocità con affidabilità. Uno strumento che aggrega decine di fonti in pochi secondi è utile per la raccolta, ma il tempo risparmiato non deve tradursi in un salto della verifica incrociata.

Perché conta, anche fuori dal lavoro investigativo

Per un giornalista o un comunicatore che deve verificare una fonte anonima prima di darle credito, questo metodo è la differenza tra una notizia solida e una smentita in redazione. Per chi lavora in una piccola organizzazione e riceve una richiesta di pagamento o un contatto commerciale sospetto, applicare anche solo il primo e il quarto passo — isolare il dato, cercare conferma indipendente — riduce concretamente il rischio di truffa. Per chiunque usi strumenti di intelligenza artificiale per riconoscere volti o testi, l'esempio di Google Lens resta il promemoria più diretto: un sistema che sbaglia non lo segnala, restituisce comunque una risposta con la stessa sicurezza di quando ha ragione.

Il criterio da portarsi a casa

La domanda giusta non è mai "cosa ha trovato lo strumento", ma "cosa conferma una seconda fonte indipendente". Se non c'è una seconda fonte, quello che hai in mano è un indizio, non un'identità.

Vale per un investigatore con vent'anni di esperienza quanto per chi controlla un profilo prima di rispondere a un messaggio: la differenza tra i due non è l'accesso a strumenti migliori, è la disciplina di non fermarsi al primo risultato.

Durante un webinar dedicato alle tecniche di investigazione OSINT, Mark Bentley — quasi quarant'anni come detective tra National Crime Agency, Metropolitan Police e Child Exploitation and Online Protection Command — ha caricato su Google Lens una propria foto scattata davanti a un'ambasciata. Il sistema ha restituito una corrispondenza: il suo volto associato al profilo di una persona ricercata. Non era lui. Era un errore del riconoscimento facciale, quella che in gergo si chiama allucinazione algoritmica: il sistema non ammette di non sapere, produce comunque una risposta plausibile.

Se capita a un professionista che sta dimostrando apposta i limiti dello strumento, immagina cosa può succedere a chi usa lo stesso strumento per farsi un'idea su uno sconosciuto — un venditore online, un profilo che chiede l'amicizia, un candidato al colloquio, un contatto di lavoro mai incontrato di persona. Un singolo risultato di ricerca per immagini, preso per buono, può trasformare un'identità sbagliata in un sospetto reale nella tua testa. Ed è esattamente il problema che la metodologia OSINT prova a risolvere: non trovare informazioni, ma [non fidarsi di una sola fonte](#) prima di trovarle davvero.

Cos'è, in pratica, un'indagine OSINT

OSINT sta per Open Source Intelligence: raccolta e analisi di informazioni disponibili pubblicamente — profili social, numeri di telefono, indirizzi email, immagini, dati di violazioni note. Non richiede accesso a sistemi privati né competenze da hacker. Richiede metodo.

Bentley riassume l'approccio in tre fasi, che vale la pena tenere a mente anche fuori dal contesto investigativo professionale, ogni volta che si prova a verificare chi c'è dall'altra parte di uno schermo.

La prima fase è il punto di partenza, il **pivot**: un solo dato iniziale, che sia un'email, un numero di telefono, un nome utente o un'immagine. Da lì si parte, non si arriva. La seconda fase è la **verifica**: nessun dato trovato online va considerato vero finché non trova un riscontro incrociato, indipendente dalla prima fonte. La terza è la **valutazione**: solo dopo aver raccolto più elementi corroborati si può costruire un quadro complessivo, e anche in quel momento resta un quadro probabile, non una certezza assoluta.

Il punto debole di questo processo, quando viene saltato, è sempre lo stesso: fermarsi al primo risultato.

Il metodo, passo per passo

Primo passo: definisci il dato di partenza e isolalo. Se hai un'email sospetta, un profilo social o un numero di telefono, prendi solo quello. Non partire già con un'ipotesi su chi sia la persona: l'ipotesi arriva dopo, dai dati, non prima.

Secondo passo: proteggi il dispositivo prima di cercare, non dopo. Ogni ricerca lascia tracce — pixel di tracciamento nascosti nelle pagine, crawler che registrano la visita, notifiche che avvertono l'account cercato che qualcuno lo sta osservando. Prima di aprire profili o siti sospetti, usa un browser con protezioni attive (opzioni "Do Not Track", blocco tracker) o una macchina virtuale se l'indagine è delicata. Nessuna di queste misure è infallibile, ma riduce il rischio di essere notati o tracciati a propria volta. Un controllo utile e gratuito: il sito tosdr.org riassume in modo leggibile cosa i termini di servizio di un'app o piattaforma dicono davvero sulla raccolta dati, evitando di doverli leggere per intero.

Terzo passo: interroga più fonti sullo stesso dato, non una sola. Un'email può essere verificata su più strumenti che controllano se compare in violazioni di dati note — [Have I Been Pwned](#) è il più conosciuto e gratuito — o se è collegata ad account su servizi specifici. Un numero di telefono può essere controllato per operatore e formato, poi incrociato con directory pubbliche per vedere se emergono nomi associati. Un'immagine va passata per una ricerca inversa (per esempio

TinEye) e, se possibile, analizzata nei metadati con uno strumento come ExifTool, che può rivelare data, dispositivo o posizione di scatto — quando questi dati non sono stati rimossi.

Quarto passo: applica la regola ABC prima di considerare un dato affidabile. Acquisisci il dato, conservane una copia (screenshot, salvataggio della pagina, non solo il link, che può sparire), e cercane conferma indipendente. Se una sola fonte dice una cosa e nessun'altra la conferma, quel dato resta un'ipotesi, non un fatto.

Quinto passo: aggrega solo dopo aver verificato, non prima. Esistono piattaforme che interrogano centinaia di database contemporaneamente per velocizzare la ricerca — durante il webinar è stata usata UserSearch come esempio, con una funzione basata su modelli linguistici (Sargebot) per incrociare frammenti di email, numero e foto in un report automatico. Questo tipo di strumento accelera la raccolta, non sostituisce la verifica: un aggregatore che restituisce dieci corrispondenze ha comunque bisogno che tu ne controlli l'affidabilità una per una, esattamente come per la singola ricerca su Google Lens dell'esempio iniziale.

Gli errori più comuni

Il primo errore è trattare un singolo risultato come una prova. È quello che è successo con Google Lens: un'associazione visiva sbagliata, presa per buona, avrebbe potuto costruire un sospetto infondato su una persona reale.

Il secondo è cercare senza pensare a chi vede la ricerca. Molti strumenti — anche quelli "innocui" come una verifica email — notificano al servizio che qualcuno ha effettuato quel controllo, o lasciano tracce che permettono di risalire a chi ha cercato. Chi indaga senza precauzioni rischia di avvisare proprio la persona che sta osservando.

Il terzo è confondere velocità con affidabilità. Uno strumento che aggrega decine di fonti in pochi secondi è utile per la raccolta, ma il tempo risparmiato non deve tradursi in un salto della verifica incrociata.

Perché conta, anche fuori dal lavoro investigativo

Per un giornalista o un comunicatore che deve verificare una fonte anonima prima di darle credito, questo metodo è la differenza tra una notizia solida e una smentita in redazione. Per chi lavora in una piccola organizzazione e riceve una richiesta di pagamento o un contatto commerciale sospetto, applicare anche solo il primo e il quarto passo — isolare il dato, cercare conferma indipendente — riduce concretamente il rischio di truffa. Per chiunque usi strumenti di intelligenza artificiale per riconoscere volti o testi, l'esempio di Google Lens resta il promemoria più diretto: un sistema che sbaglia non lo segnala, restituisce comunque una risposta con la stessa sicurezza di quando ha ragione.

Il criterio da portarsi a casa

La domanda giusta non è mai "cosa ha trovato lo strumento", ma "cosa conferma una seconda fonte indipendente". Se non c'è una seconda fonte, quello che hai in mano è un indizio, non un'identità. Vale per un investigatore con vent'anni di esperienza quanto per chi controlla un profilo prima di rispondere a un messaggio: la differenza tra i due non è l'accesso a strumenti migliori, è la disciplina di non fermarsi al primo risultato.