

Mettiamoci la faccia

Milano, notte di Capodanno. Piazza Duomo e dintorni sono gremiti da persone scese in strada a festeggiare. Tra la folla però sta accadendo qualcosa di terribile e inaspettato: alcune ragazze sono oggetto di violenza sessuale da parte del “branco” che, complici i rumori tipici dell’ultima notte dell’anno, porta a termine le proprie scellerate azioni. Ci sono però degli occhi attenti che hanno visto tutto e che non dimenticano alcun particolare: le telecamere puntate sulla piazza. Gli investigatori della Squadra mobile e del commissariato “Centro” si coordinano con l’autorità giudiziaria e sequestrano le immagini riprese e quelle presenti sui social relative all’evento. A Milano, al Gabinetto regionale della polizia scientifica diretto da Annamaria Di Giulio, si analizza il materiale che porterà a svelare l’identità dei responsabili, riconosciuti poi dalle vittime di quegli atti vili. «Noi lavoriamo sempre con le immagini originali – dice Lorenzo Rinaldi, direttore della IV divisione del Servizio polizia scientifica – e chiediamo agli uffici investigativi di non rielaborarle o modificarle. Abbiamo costruito una rete informatica distribuita su tutto il territorio nazionale e non c’è quindi più bisogno che queste immagini viaggino su supporti come chiavette usb o dvd. Ogni questura e ogni Gabinetto regionale di polizia scientifica dispone di proprie cartelle informatiche condivise che gli permettono di trasmetterci materiali in modo sicuro e senza alcuna perdita di qualità. Una volta ricevute le immagini operiamo una valutazione sulla qualità e le miglioriamo, cercando di superare i limiti dettati dalla risoluzione o dalla scarsa illuminazione, utilizzando dei software specifici che ne riducano il “rumore”, esaltando il contenuto informativo. Stiamo puntando molto su algoritmi di intelligenza artificiale».

Spesso però il volto ripreso dalle telecamere non è “noto” alle forze dell’ordine e ciò accade quando il soggetto non sia stato già “fotosegnalato” in precedenza, operazione alla quale possono essere sottoposte, se necessario, le persone nei cui confronti vengono svolte le indagini (ex art. 349 co 2 del cpp) e quelle pericolose o sospette nonché coloro che non sono in grado, o si rifiutano, di provare la loro identità (ex art. 4 Tulps).

«La banca dati che viene interrogata per il riconoscimento facciale – sottolinea Rinaldi – è quella dell’Afis, *Automated fingerprint identification system* (Sistema automatizzato di identificazione delle impronte digitali), che contiene foto di oltre 10milioni di soggetti diversi, perché l’autorizzazione ottenuta dall’Autorità garante per la protezione dei dati personali è relativa esclusivamente alla ricerca nelle banche dati degli individui fotosegnalati dalle forze di polizia. Spesso ci viene chiesto se le foto utilizzate per il rilascio del passaporto o della carta d’identità vengano inserite in questo archivio. La risposta è negativa perché qui, oltre ai dati dei soggetti fotosegnalati per i motivi sopra elencati, confluiscono solo quelli degli immigrati regolari, secondo la legge Bossi-Fini che prevede il fotosegnalamento di chi richiede il permesso di soggiorno, irregolari e di coloro che chiedono la protezione internazionale, come previsto da un regolamento europeo».

Il Sari enterprise Il sistema utilizzato dalla Scientifica per il riconoscimento delle immagini è il “Sari” (Sistema automatico di riconoscimento immagini) che rappresenta una delle più grandi innovazioni degli ultimi anni. Utilizzato su larga scala per il riconoscimento dei volti dal 2018, è diventato un aiuto sempre più prezioso nelle indagini. Col crescere del numero delle telecamere installate nelle città, negli esercizi commerciali e nei condomini, è infatti cresciuto anche il numero degli atti criminali, e dei relativi autori, che sono stati ripresi. Fondamentale, però, rimane nell’analisi la competenza dell’operatore: «L’esperienza e la formazione di colui che effettua la ricerca e la comparazione di immagini – prosegue Rinaldi – ha un’importanza assolutamente rilevante. Il sistema non è automatico, e d’altronde non potrebbe esserlo, ed effettua la ricerca, grazie ad algoritmi di intelligenza artificiale, in maniera davvero veloce ed efficace, realizzando un’attività che sarebbe impossibile svolgere manualmente. Una volta che analizza immagini con sufficienti requisiti di qualità, e riprese con una determinata inquadratura e angolazione, il sistema cerca nella banca dati dell’Afis e propone all’operatore un elenco di candidati compatibili con l’immagine o il video analizzati. Qui entra in gioco l’abilità dell’operatore, perché ad ogni candidato è associato uno “score” (punteggio) che rappresenta una misura di somiglianza fornita dal sistema. Ovviamente l’operatore partirà dalle immagini che hanno uno “score” più alto ma su queste applica le procedure di comparazione sulle quali è stato debitamente formato e solo questa formazione lo porterà a dire se il soggetto potrebbe essere o meno quello ricercato. Va poi ricordato che i risultati ottenuti sono di tipo “investigativo” e non “forense” e servono ad evidenziare un sospettato e a farlo sottoporre ad altri accertamenti come un pedinamento o un confronto con testimoni. Nel caso di Milano, ad esempio, il sistema ha estrapolato dei volti, ma a

queste indicazioni è seguita un'importante attività di indagine. Sintetizzando quindi, potrei dire che si parte da un volto ignoto, si ricerca nel *Sari* con un operatore esperto e se ne ricava uno spunto investigativo».

L'interscambio con enti e università Il *Sari* usa due sistemi di riconoscimento facciale, due motori di ricerca basati sull'intelligenza artificiale e la scelta di questi motori non è di tipo "autoreferenziale". Le performance sono, infatti, testate dal Nist, *National institute of standards and technology*, ente statunitense che esamina i migliori algoritmi mettendoli a confronto e valutandone i risultati. Quelli utilizzati dalla Scientifica sono tra i più efficienti al mondo e vengono costantemente aggiornati. Il rapporto con le università, con il Cnr e con l'Enea è proficuo e costante e gli accordi di collaborazione stipulati permetteranno di testare i numerosi algoritmi di riconoscimento immagini da questi sviluppati. Il punto di forza della Scientifica infatti, oltre all'esperienza degli operatori, è il grande archivio dati delle forze di polizia, all'interno del quale effettuare prove e ricerche senza trasmettere dati sensibili all'esterno. Evidenziare gli algoritmi più efficaci è importante non solo per chi li ha prodotti ma anche per le forze di polizia che, una volta validati e commercializzati, potranno utilizzarli nelle indagini sul campo.

Sicurezza vs privacy Il *Sari* è un sistema composto da due diverse infrastrutture, parallele ma separate: *Sari enterprise* e *Sari real time*. Quest'ultimo è in grado, automaticamente e in tempo reale, di confrontare i volti inquadrati dalle telecamere con una lista contenente quelli delle persone da ricercare (*watch list*). Se il volto è presente nella lista, il sistema lancia un *alert* e lo segnala così all'operatore addetto al controllo. Il sistema, progettato e sviluppato come soluzione mobile, può essere installato direttamente presso il luogo ove sorga l'esigenza di disporre di una tecnologia di riconoscimento facciale per coadiuvare le forze di polizia nella gestione dell'ordine e della sicurezza pubblica, o in relazione a specifiche esigenze di polizia giudiziaria. Sull'utilizzo del *Sari enterprise* si è pronunciato favorevolmente il Garante per la protezione dei dati personali nel 2018. Per quanto riguarda, invece, l'utilizzo del *Sari real time*, attesa la maggiore "invasività" del sistema, prima di concederne l'autorizzazione, il Garante ha richiesto che fosse redatta una valutazione d'impatto sulla protezione dei dati personali. La valutazione è stata inviata al Garante che però, con nota del 16 aprile 2021, ha espresso parere negativo alla messa in opera del sistema, vista, sostanzialmente, la mancanza di una adeguata base normativa che ne consentisse l'utilizzo. Il *Sari real time* non è, quindi, mai entrato in uso. Considerata l'attualità della tematica dei sistemi di controllo in tempo reale, un ampio dibattito si è tenuto anche all'interno delle Istituzioni dell'Unione europea che, ad oggi, stanno lavorando alla redazione di un "Artificial intelligence act", un regolamento generale sull'uso dei sistemi basati sull'intelligenza artificiale che ne disciplini tutti gli aspetti legati alla vita sociale e all'utilizzo da parte delle forze di polizia; l'attuale bozza di regolamento prevede che queste possano utilizzarli in specifiche attività, come la ricerca di vittime di crimini, la prevenzione di minacce imminenti alle infrastrutture critiche o in caso di attacchi terroristici, introducendo però una serie di garanzie per i cittadini come la necessità di autorizzazione da parte dell'autorità giudiziaria e l'utilizzo in aree definite e per tempi limitati.

«In attesa dell'approvazione della normativa europea – sottolinea Rinaldi – va però notato che la legge n. 205 del 3 dicembre 2021, all'articolo 9, introduce delle modifiche al codice per la protezione dei dati personali trattando, specificatamente, l'utilizzo di impianti di videosorveglianza, in luoghi pubblici o aperti al pubblico, con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici. La normativa ne sospende l'utilizzo fino all'entrata in vigore di una disciplina legislativa della materia e, comunque, non oltre il 31 dicembre 2023. Tuttavia sono previste delle eccezioni (consentendone quindi l'utilizzo, *ndr*) per i trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati in presenza, salvo che relativamente a trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante. Si sta quindi valutando di presentare una nuova interrogazione al Garante, alla luce dei recenti risvolti normativi, così che possa esprimere parere positivo all'utilizzo del *Sari real time*».

Il prossimo futuro «Stiamo investendo nello studio della *gait recognition* – conclude Rinaldi – ossia il riconoscimento potenziale delle persone in base alla loro andatura, perché questa è tipica e particolare in ogni persona. Lo studio biometrico si basa su conoscenze che l'uomo ha sempre avuto, poiché è naturalmente in grado di riconoscere le persone in base a questa caratteristica, basti pensare all'espressione "ti ho riconosciuto da lontano da come camminavi" che è di uso comune. Oggi la tecnologia è pronta ad aiutarci e sono allo studio algoritmi che, in un prossimo futuro, ci permetteranno di essere di supporto alle indagini anche in questo campo. Le applicazioni potenziali sono molte e si riferiscono a tutte quelle situazioni nelle quali un video "catturi" la camminata di un soggetto responsabile di un reato. Non siamo ancora pronti, ma lo studio è iniziato. Anche qui l'intelligenza artificiale sarà di grande aiuto».

Quando le indagini diventano elettroniche Le indagini elettroniche hanno come obiettivo quello di seguire e/o raccogliere le numerosissime tracce elettroniche che oggi ognuno di noi lascia dietro di sé e, di conseguenza, che vengono lasciate anche sulla scena del crimine. Queste fanno riferimento all'insieme delle tecnologie che permettono di catturare, ricercare ed estrarre le cosiddette "digital evidence", contenute in dispositivi fisici o virtuali, connesse ad una scena del crimine, ad un luogo o ad un evento di interesse investigativo. Molto diversificati sono gli accertamenti tecnici e forensi che rientrano nell'alveo delle indagini elettroniche (confronto forense del volto, riconoscimento facciale mediante sistemi automatizzati, confronto forense del parlatore, miglioramento di immagini, ecc.) e tutti fanno uso della migliore tecnologia messa a disposizione dalla ricerca scientifica e recentemente anche di algoritmi di intelligenza artificiale. *Francesco Sherborne*

Imparare a comparare La Scientifica ha redatto un manuale sulle "linee guida per il confronto fisionomico", accertamento tecnico per la comparazione di volti raffigurati in immagini che ha lo scopo di stabilire il livello di corrispondenza tra le immagini del volto di un soggetto di interesse e con identità ignota, rispetto alle immagini del volto di un sospettato con identità, in genere, nota oppure anch'essa ignota. Il confronto è eseguito manualmente dall'operatore che, attraverso l'utilizzo della comparazione morfologica, analizza le immagini ritraenti i volti in esame. Il manuale, che riporta anche le *best practice* sul tema acquisite in gruppi di lavoro europei, è stato distribuito agli Uffici di polizia.

09/03/2022