PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4372 di Venerdì 14 dicembre 2018

Il riconoscimento facciale nelle indagini delle forze dell'ordine

Le tecnologie usate dai sistemi di riconoscimento facciale per analizzare riprese video, relative ad eventi criminosi, per cercare di individuare i colpevoli, hanno destato l'attenzione dei tutori della protezione dati personali.

La crescita esponenziale degli impianti di videosorveglianza fa sì che sempre più spesso, in concomitanza con la perpetrazione di un reato, le forze dell'ordine abbiano a disposizione numerose videoregistrazioni, che possono inquadrare la scena del crimine o le aree immediatamente circostanti.

L'utilizzo di queste videoregistrazioni può essere prezioso per ricostruire non solo le modalità dell'evento criminoso, ma anche aiutare ad identificare i soggetti coinvolti. In Inghilterra, recentemente, una associazione, che tutela il diritto alla privacy dei cittadini, si è rivolta all'Alta corte di giustizia, perché riteneva che la polizia utilizzasse in modo non appropriato applicativi di riconoscimento automatico dei voti. Inoltre, a livello europeo, si sta creando un archivio di volti, che sotto certi aspetti ricorda da vicino l'archivio delle impronte digitali, che oggi vengono analizzate e confrontati in forma automatica, non solo a livello europeo, ma anche in collaborazione con paesi esterni All'unione europea.

La nostra autorità Garante si è pronunciata il 26 luglio 2018 su questo tema, che è stato affrontato anche da altre autorità Garanti. A questo punto, è bene ricordare che l'entrata in vigore del nuovo regolamento europeo fa sì che non sia possibile a due autorità Garanti, presenti in due diversi paesi europei, di esprimersi in modo difforme su temi analoghi. Se ciò accade, si deve ricorrere al Comitato europeo per la protezione dei dati, che emetterà un giudizio finale.

Prima di affrontare questo problema, vediamo quali sono le modalità di utilizzo più frequente di questi applicativi.

Tanto per cominciare, una recente ricerca di mercato ritiene che il volume di affari, legato all'utilizzo di questi applicativi, salirà da 4 miliardi di dollari nel 2017 a 8 miliardi di dollari nel 2022. Ciò premesso, vediamo possibili applicazioni.

Appare evidente che una prima possibile applicazione è quella di accelerare il confronto fra le immagini provenienti da numerose videoregistrazioni, per identificare, nelle varie immagini, dei volti che si ripetono in modo sistematico.

Quando le forze dell'ordine hanno a disposizione dozzine di video registrazioni, è evidente che effettuare questa operazione manualmente richiede un tempo straordinariamente elevato ed è quindi necessario utilizzare potenti strumenti informatici, in grado di automatizzare l'analisi delle immagini ed individuare le somiglianze tra i volti.

Il fatto di accelerare questa fase può aiutare le forze dell'ordine a intervenire più tempestivamente, successivamente al crimine, per mettere sotto controllo la situazione.

È bene comunque sottolineare che gli strumenti software mettono a disposizione informazioni, che devono però essere convalidate da un esperto. Inoltre, queste immagini non possono essere utilizzate come prova, ma solo come indizio che può guidare successive indagini.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[SWGDPR] ?#>

Un altro utilizzo frequente, soprattutto negli Stati Uniti, è legato al fatto che la polizia potrebbe fermare un soggetto, alla guida di un'autovettura. Il soggetto non ha documenti d'identità e dovrebbe essere possibile, rapidamente, catturare un'immagine del suo volto ed effettuare una analisi per confronto con una banca dati, per vedere se per esempio ci si trova davanti a un soggetto che non ha rispettato gli obblighi di soggiorno obbligato, oppure è ricercato per altri motivi.

Infine, non dimentichiamo che il riconoscimento facciale può essere utilizzato anche per ragioni umanitarie. Ad esempio, il riconoscimento facciale può aiutare ad identificare dei cadaveri, privi di documenti di identità. In altri casi, questi applicativi permettono di aiutare ad identificare un soggetto, che per varie ragioni, come ad esempio per il fatto che egli è affetto da Alzheimer, non ricordi chi sia e dove abiti.

Una gran parte delle contestazioni che vengono fatte questi applicativi riguarda l'accuratezza del riconoscimento e soprattutto il fatto che questi applicativi potrebbero identificare non correttamente una persona innocente. Ecco la ragione per la quale ogni risultato dell'applicazione di questi dispositivi di riconoscimento facciale deve essere attentamente analizzato da un esperto, che possa convalidare il livello di qualità della identificazione.

Un altro aspetto al quale occorre prestare molta attenzione riguarda il fatto che l'algoritmo non deve essere articolato in modo da dare un peso specifico differenziato a caratteristiche particolari, come ad esempio la razza o il sesso del soggetto che si sta analizzando.

A questo proposito, gli esperti ritengono che le forze dell'ordine dovrebbero dare ampia pubblicità a questi applicativi, illustrando alla popolazione le modalità con cui funzionano e le modalità con cui vengono applicati, in modo da diminuire i ragionevoli turbamenti della popolazione, in termini di possibile violazione del loro diritto alla protezione dei dati.

Un altro aspetto da esaminare attentamente riguarda le modalità con cui viene creata una banca dati, da utilizzare per i confronti fra i volti catturati, ad esempio, sulla scena del crimine e l'archivio generale. Tutti gli esperti sono concordi nell'affermare che non deve essere assolutamente possibile utilizzare, ad esempio, la base dei dati con le fotografie di coloro che hanno richiesto una patente oppure una carta di identità, perché la base dei dati sarebbe troppo grande e le possibilità di identificazione errate sarebbero altrettanto elevate.

Ecco perché gli esperti ritengono che solo volti di soggetti che hanno precedenti storie giudiziarie dovrebbero essere inseriti in questi archivi. In sintesi, questi applicativi possono essere preziosi ma richiedono ancora esperienze studi approfonditi sulle modalità di utilizzo.

La situazione in Italia ed il parere del Garante

Il nostro Garante si espresso sul tema con un provvedimento "Sistema automatico di ricerca dell'identità di un volto - 26 luglio 2018".

Il Ministero dell'Interno sta predisponendo un sistema automatico di ricerca dell'identità di un volto presente in un'immagine all'interno di una banca dati, denominato "SARI Enterprise".

In riscontro alla richiesta di chiarimenti del Garante, il Ministero ha precisato che il sistema è destinato ad affiancare il sistema AFIS-SSA, per fornire all'operatore un efficiente supporto informatico che ne agevoli l'attività di indagine.

Il sistema AFIS-SSA, attualmente in uso, consente di effettuare ricerche nell'archivio dei soggetti fotosegnalati (A.F.I.S.), tramite l'opera manuale di un operatore, che deve inserire nei campi presenti nella maschera di interrogazione informazioni anagrafiche, connotati e contrassegni (ad esempio, colore dei capelli, degli occhi, di tatuaggi), al fine di individuare la presenza nell'archivio AFIS del soggetto ricercato.

Il data base AFIS ed il sistema AFIS-SSA sono previsti nel decreto del Ministro dell'interno 24 maggio 2017, recante l'individuazione dei trattamenti di dati personali effettuati dal Centro elaborazione dati del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'art. 53, comma 3, del decreto legislativo 30 giugno 2003, n. 196, la cui scheda 19 contiene la descrizione del sistema e indica le numerose fonti normative di riferimento, di rango legislativo e regolamentare.

Il sistema SARI Enterprise, di prossima attivazione, non effettuerà elaborazioni aggiuntive rispetto al AFIS-SSA, ma si limiterà ad automatizzare alcune operazioni che prima richiedevano l'inserimento manuale di connotati identificativi, consentendo le operazioni di ricerca nel data base dei soggetti fotosegnalati attraverso l'inserimento di una immagine fotografica, che sarà elaborata automaticamente al fine di fornire l'elenco di foto segnaletiche somiglianti, ottenute attraverso un algoritmo decisionale che ne specifica la priorità.

Pertanto, l'utilizzo del sistema SARI-Enterprise costituisce non un nuovo trattamento di dati personali, già previsto e disciplinato dalle predette fonti, bensì una nuova modalità di trattamento di dati biometrici, che dovrà essere effettuata nel rispetto delle regole previste dalla normativa rilevante in materia di tutela dei dati personali.

Infine, cinque passi per un'applicazione corretta di questi applicativi

Un esperto americano, che da anni opera in questo settore, ha messo a disposizione una procedura, articolata in cinque passi, che permette alle forze dell'ordine di utilizzare al meglio questi applicativi, senza incidere in maniera anomala sui diritti dei cittadini potenzialmente coinvolti.

1-Identificare l'immagine. Un poliziotto esperto deve porsi le seguenti domande, quando analizza le immagini per verificarne la qualità:

- l'immagine soddisfa i criteri minimi necessari per utilizzare un applicativo di riconoscimento facciale?
- l'immagine ha bisogno di manipolazioni reversibili?
- l'immagine viene rifiutata dall'applicativo?

Se si verificano questi eventi, occorre introdurre dei filtri sui dati per restringere il campo di ricerca e mettere a disposizione un numero di possibili coincidenze ragionevolmente gestibile.

2-Avviare la ricerca.

3-L'identificazione facciale. È normale che delle immagini di bassa qualità possano presentare all'operatore parecchie centinaia di volti, che potenzialmente potrebbero corrispondere a quello in esame. Quando si verifica questa situazione, l'operatore deve analizzare alcune delle immagini presentate, che gli sembrano essere più vicine a quella del soggetto ricercato, ed introdurre delle limitazioni nella ricerca, che possano ridurre in maniera significativa il numero delle opzioni presentate.

4-Effettuare una verifica dei risultati della ricerca. Vi sono due livelli di verifica:

- la verifica di primo livello, alla fine della quale vi è una ragionevole probabilità che i volti presentati possano appartenere al soggetto ricercato; occorre allora avviare subito una ricerca per raccogliere elementi ulteriori di filtraggio, come ad esempio il fatto che il soggetto in questione potrebbe essere in prigione, e quindi non deve essere preso in considerazione, oppure potrebbe abitare distanza dal luogo dove si è verificata la scena in esame. L'acquisizione della storia criminale dei soggetti, potenzialmente riconducibili al soggetto ricercato, aiuta certamente nel restringere il numero dei soggetti stessi.
- la verifica di secondo livello invece prevede che gli esiti di questa analisi vengano presentati a due o tre persone, anch'essi appartenenti alle forze dell'ordine, per ottenere un giudizio indipendente circa la validità della ricerca.

5-Infine si passa all'ultimo punto, ricordando che comunque i risultati della ricerca facciale sono soltanto degli indizi investigativi, e non sono prove. Nessuno dovrebbe essere arrestato solo per il fatto che il sistema di analisi del riconoscimento facciale indica una elevata probabilità di coincidenza.

L'applicativo del riconoscimento facciale serve quindi a guidare l'operato delle forze dell'ordine e non deve essere utilizzato come unico strumento di indagine.

Allegato provv garante (PDF)

Adalberto Biasiotti
