PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3811 di martedì 28 giugno 2016

Il riconoscimento automatico facciale

Sono pochi i lettori che sanno fino a che punto è stata sviluppata la tecnologia di riconoscimento facciale negli Stati Uniti e come essa viene già utilizzata su larga scala. Il punto sulla situazione e alcuni problemi sono già apparsi. Di A. Biasiotti.

Già dal 2011 il Federal Bureau of investigations aveva impostato un programma di riconoscimento facciale, con l'obiettivo di aiutare gli investigatori e le forze dell'ordine nell'effettuare un confronto, in parte automatizzato, fra le immagini, ad esempio catturate da un impianto di videosorveglianza, ed un archivio di volti, che nasce da precedenti indagini, da soggetti incarcerati, da fotografie associate al rilascio della patente e del passaporto e da altre basi di dati, dove sono presenti fotografie di soggetti non necessariamente criminali.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[DVD032] ?#>

Il dipartimento della giustizia ha quindi messo a punto questo programma, che viene chiamato con i soliti acronimi anglosassoni NGI-IPS, che significa Next generation identification-interstate photo system.

La base dei dati ad oggi già archivia la bellezza di 411 milioni di fotografie, provenienti, come accennato, da un gran numero di basi dei dati.
L'accesso a questo sistema di riconoscimento facciale è consentito ovviamente agli agenti dell'FBI ed altre forze di polizia, dove sono presenti funzionari particolarmente addestrati.
Questi soggetti possono quindi presentare una richiesta di analisi di un volto, per qualsiasi ragione coinvolto in possibili attività criminose, chiedendo di effettuare un controllo automatico di corrispondenza con voti già archiviati.

Il sistema automatizzato è in grado di mettere a disposizione una lista di possibili soggetti, che può essere allargata o ristretta, in funzione delle richieste della agenzia richiedente.
Per solito la lista varia da due a 50 possibili soggetti, estratti da una base dei dati.
A dicembre 2015, l'FBI aveva degli accordi con sette Stati e altri Stati vengono aggiunti, non appena vengono superati i controlli e le garanzie incrociate di corretto ed efficiente utilizzo del sistema.
Per migliorare ancora di più le caratteristiche di questo sistema, lo FBI ha creato al suo interno un squadra specializzata, chiamata con il nuovo acronimo di FACE-facial analysis, comparison and Evaluation. Questo servizio offre un'integrazione visiva, sviluppata da tecnici specializzati, che analizzano i risultati del riconoscimento automatico dei volti, effettuando un ulteriore filtro. Questi analisti biometrici esaminano quindi ogni singola fotografia estratta automaticamente dal sistema e mettono a disposizione al massimo uno o due fotografie. È importante ridurre al minimo il numero delle fotografie che vengono offerte agli organi investigativi per evitare di disperdere le forze e soprattutto per evitare che soggetti innocenti, che hanno l'unica colpa di assomigliare ad un volto criminale, vengano coinvolti nelle indagini.

D'altro canto, una ristrettezza eccessiva della lista può avere delle controindicazioni, perché potrebbero essere eliminati dalla lista dei volti, che invece potrebbero proprio corrispondere a criminali coinvolti.

Appare evidente che un sistema di questo genere può essere gravemente invasivo nei confronti della protezione dei dati personali ed ecco perché sin dal 2008 è stato imposto alla dipartimento di giustizia di sviluppare una valutazione di impatto sulla privacy, che è in tutto uguale a quella che viene richiesta dal nuovo regolamento europeo 2016/679, per trattamenti particolarmente invasivi.
Gli ispettori che hanno analizzato questo sistema di riconoscimento facciale hanno potuto accertare che questa valutazione di impatto sulla privacy non è stata condotta in modo appropriato e soprattutto non è stata aggiornata quando il sistema è stato

modificato in modo radicale, introducendo appunto una unità ausiliaria di valutazione, chiamata FACE.

Ecco la ragione per la quale molti difensori della privacy, negli Stati Uniti, sono entrati in allarme e hanno chiesto che possano essere offerte al pubblico delle garanzie appropriate che il sistema venga utilizzato nel pieno rispetto delle esigenze delle forze dell'ordine, ma anche delle esigenze di tutela della privacy di tutti i cittadini americani, le cui fotografie sono inserite nel sistema.

Può essere interessante per i lettori sapere anche quale è il grado di affidabilità di questi sistemi automatizzati. A questo proposito l'FBI ha sviluppato una serie di verifiche per vedere se questi sistemi automatici sono in grado di estrarre correttamente dalla base dei dati i volti che più assomigliano a quelli sottoposti ad esame. Gli esiti di questa indagine non sono stati resi pubblici e ciò fa ritenere che possano non essere particolarmente brillanti.

D'altro canto, se si estende fino a 50 l'elenco dei volti che possono essere estratti dal confronto ci si rende conto che il sistema potrebbe non essere così utile come si pensa, anche se certamente è meglio approfondire l'investigazione nei confronti di 50 soggetti, piuttosto che di 300.000.000 di cittadini americani.

Sulla base delle esperienze passate, si può tuttavia affermare che questi sistemi, che inizialmente avevano lasciato molti dubbi circa la loro efficienza ed efficacia, col passare del tempo possono solo migliorare, grazie all'evoluzione degli algoritmi di confronto ed ad altri interventi, che l'esperienza indica come utili per un miglioramento dei risultati.

Alla fine dell'indagine, gli ispettori hanno avanzato la bellezza di sei raccomandazioni, alcune molto incisive, in parte afferenti alla protezione dei dati personali ed in parte afferenti alle modalità di gestione del sistema e accesso ai dati.

Ai lettori che si chiedono come mai questo sistema, seppur non perfetto, non potrebbe essere utilizzato anche in Italia, a sostegno dell'indagine delle forze dell'ordine, rispondo che non ho alcuna notizia circa una iniziativa in questo senso da parte del ministero dell'interno.
Ad oggi, l'unico sistema automatizzato è quello relativo all'incrocio delle impronte digitali, il cosiddetto sistema AFIS-automatic Fingerprint identification system, che ha comunque dato risultati eccezionalmente positivi.

È ben vero che vi è una grossa differenza fra una verifica di una impronta digitale e la c, ma gli algoritmi diventano sempre più intelligenti e potranno quindi in un futuro, forse non lontano, aiutare le forze dell'ordine nella lotta contro la criminalità.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it