In difesa della tecnologia del riconoscimento del volto

Contro il *face detection ban*

Sommario

1) Premessa 2
2) Il dibattito sul riconoscimento facciale 3
3) Quando la biometria del volto è inutile 4
4) Quando la biometria del volto è utile 6
a) Segue: i sistemi online nelle videosorveglianze in luoghi pubblici 7
5) Le cautele per evitare abusi 9
a) Segue: sempre sulle misure di sicurezza 10
6) Gli effetti sull'industria europea dell'eventuale *facial recognition ban* 11
7) Conclusioni 12

Indice delle figure

Figura 1: Il Progetto Interpol MI-LEX 6

1) Premessa

Notizie diffuse da organi di stampa internazionali (qui e qui), poi riprese da quelli italiani (qui e qui), riportano che l'Unione Europea starebbe considerando di vietare l'impiego delle tecnologie di riconoscimento facciale negli spazi pubblici (che, nella terminologia del Vecchio Continente, riguarda anche gli spazi aperti al pubblico), per tre o cinque anni.

Quanto sopra, a seguito di alcune vicende avvenute di recente, che hanno fatto scattare l'allarme sulla biometria del volto, che si illustrano al par. 2).

L'ipotesi è contenuta in una la bozza di un white paper della Commissione Europea, che A.I.PRO.S. è in grado di mettere a disposizione dei lettori, in materia di Intelligenza Artificiale.

La Commissione riterrebbe che, durante questo lasso di tempo, potrebbe essere sviluppata una solida metodologia per valutare l'impatto e le possibili misure di gestione dei rischi.

2) Il dibattito sul riconoscimento facciale

L'impiego del riconoscimento facciale ha portato a un grande dibattito negli Stati Uniti e in Europa.

In California e in altre località (qui e qui) è stato bandito l'utilizzo del riconoscimento del volto a livello cittadino o statale.

Si noti che, a livello federale, la biometria del volto continua ad essere applicata, senza obiezioni.

Nel Regno Unito, la scorsa estate, è sorto un grande dibattito in relazione alla scoperta, o alla conferma, che le forze di Polizia (che sono organizzate su base locale) utilizzano tali tecnologie.

In particolare, un pronunciamento dell'Alta Corte del Galles ha avallato l'impiego generalizzato e preventivo del riconoscimento del volto, sollevando una levata di scudi dell'ICO (il Garante della Privacy britannico), che ha rivendicato la competenza sulla materia e avvisato sui rischi esistenti in materia.

Quasi contemporaneamente, si è scoperto (qui e qui) che, a Londra, la Metropolitan Police ha impiegato la biometria facciale, anche utilizzando impianti privati. Gli accertamenti effettuati hanno dimostrato che gli esiti dell'impiego di detta tecnologia sono stati molto deludenti e hanno generato una sensibile mole di falsi allarmi (in pratica, significa che cittadini onesti possono essere scambiati come terroristi o criminali), sollevando legittimi dubbi. Di nuovo, l'ICO è intervenuta segnalando la necessità di interventi regolatori urgenti (qui).

Nel contempo, le autorità della Privacy svedese, prima, e francese, poi, hanno vietato il riconoscimento facciale (qui e qui), quest'ultimo utilizzato come controllo presenze o accessi nelle scuole.

E' noto che in diversi stati e, soprattutto, in Cina, il riconoscimento facciale viene utilizzato intensivamente e pervasivamente (qui).

Tuttavia, non c'è alcuna indicazione sull'efficacia di tale tecnologia applicata agli spazi pubblici, anche perché è difficile credere che i ripetuti fallimenti tecnologici avvenuti in Occidente possano semplicemente tramutarsi in successi in Cina.

3) Quando la biometria del volto è inutile

Chi ha seguito i recenti corsi su Videosorveglianza e Privacy, che ho tenuto a dicembre scorso, sa che nella sezione dedicata alla biometria ho criticato fortemente l'impiego generalizzato del riconoscimento del volto associato alle telecamere e ho spiegato perché, sotto il profilo tecnologico, si presentano importanti problematiche che rendono molto difficile farlo funzionare correttamente, soprattutto per la sorveglianza nei luoghi pubblici.

Alcuni di questi aspetti sono oggettivamente ineludibili, quali la distanza e l'angolazione della ripresa, la distorsione determinata da alcune tipologie di lenti e obiettivi, la luce variabile, il normale impiego di accessori sul volto (occhiali marcati, sciarpe, berretti, orecchini ingombranti, il piercing, il trucco pesante, ecc.), e altri fattori variabili (brufoli, nei, barba, baffi e capelli), anche a prescindere da un uso malizioso di camuffamenti.

Altri sono solo parzialmente rimediabili, con un rilevante (a volte: gigantesco) impiego della tecnologia e delle procedure, quali il passaggio al 3D, il dettaglio della ripresa anche a distanza, la moltiplicazione dei punti di ripresa da più angolazioni, l'aggiunta di variabili multibiometriche (trama della pelle, postura), il miglioramento e potenziamento delle capacità di processamento e l'aggiornamento continuo dei template di confronto con immagini aggiornate (infatti, l'invecchiamento del volto, rispetto ai "modelli" a suo tempo rilevati per il confronto, incide negativamente sul riconoscimento del volto), nonché il miglioramento degli algoritmi di riconoscimento (gli algoritmi esistenti mostrano scarsa capacità di elaborare le variabili morfologiche delle differenti razze e dei due sessi, sì che ogni software risulta più performante con alcune tipologie di razze, o di sesso, e meno con altre).

A fronte di queste problematiche, è lecito, anzi, necessario, interrogarsi sulle conseguenze in materia:

- di tutela dei diritti e delle libertà degli esseri umani;
- sul rapporto costi (alti) / efficienza (scarsa).

Circa la Privacy, credo che nessuno gradirebbe di essere ripetutamente fermato (magari con le armi puntate addosso), solo perché un algoritmo lo scambia per un noto terrorista e, pertanto, è stato trattato con le, rudi, cautele del caso.

Se, poi, l'algoritmo si sbagliasse con maggiore frequenza nei confronti di una razza, o di un sesso, per semplici problematiche di scarsa capacità tecnica del software, ne deriverebbero dei leciti dubbi sul rispetto del principio di eguaglianza.

Tanto più, perché l'impiego di questa tecnologia richiedere un enorme dispendio di mezzi, non solo in termini economici, ma anche di risorse umane (spesso altamente specializzate), destinate a fare funzionare e tenere continuamente aggiornato il riconoscimento facciale e, poi, a verificare gli allarmi pervenuti.

Quindi, è assolutamente lecito porre in guardia chiunque dall'impiego non corretto del riconoscimento facciale, spesso spacciato come una soluzione facile, anche se sostenuto da scarse basi scientifiche e fattuali, da fornitori di ogni tipo.

Purtroppo, una falsa, aprioristica, messianica fiducia, alimentata dalla infinità di filmetti e polizieschi che consumiamo ogni giorno, spinge continuamente i decision maker (inclusa la nostra classe politica, senza eccezioni), a scelte non razionali.

4) Quando la biometria del volto è utile

Va intanto precisato che il riconoscimento del volto è senza dubbio efficace (seppure non scevro di errori) in due circostanze:

- controlli di frontiera e in altri simili casi, quindi in aree pubbliche, ma con accesso collaborativo e controllato;
- controlli offline, con la ricerca di un volto di riprese registrate, particolarmente utili per gli organi di Polizia in aree pubbliche.

Casi di utile utilizzo dei sistemi biometrici sono riconducibili a diverse tipologie e contesti (ad es.: qui, qui e qui).

Ad esempio, proprio in relazione a queste due casistiche, l'Interpol ha varato il Progetto FIRST (*Facial, Imaging, Recognition, Searching and Tracking*), diretto al riconoscimento di criminali e terroristi al passaggio delle frontiere o in varchi di altro genere, ovvero in altre casistiche utili per il riconoscimento facciale. I risultati sono sotto gli occhi di tutti (qui, qui e qui).

In relazione al tema dei *foreign fighters* (che ci riguarda da vicino), sempre l'Interpol ha varato il programma MI-LEX (in realtà una serie di progetti realizzati con stati in particolare difficoltà), che prevede il trasferimento dei dati biometrici ai DB del Bureau, acquisiti presso le forze armate dei paesi aderenti.

Figura 1: Il Progetto Interpol MI-LEX

Quindi, il progetto mira a consentire l'individuazione di soggetti già schedati in quanto combattenti in zone di insorgenza nelle aree di conflitto, che però non risultano altrettanto schedati come terroristi dalle Forze di Polizia di paesi diversi.

E' evidente a tutti la rilevanza dell'impiego di questa tecnologia, soprattutto in termini di contenimento del rischio di trasferimento di questi soggetti in Europa, magari come clandestini (qui, qui e qui).

Si tenga presente che anche il Garante della Privacy italiano non ha avuto nulla da obiettare (qui), rispetto a un similare progetto nazionale, ancorchè di respiro più limitato.

a) Segue: i sistemi online nelle videosorveglianze in luoghi pubblici

Si potrebbe sostenere che la misura di sospensione proposta dalla Commissione riguarderebbe solo i sistemi di riconoscimento online installati sugli impianti di videosorveglianza e operativi in aree pubbliche, che effettuano la ricerca "random" dei volti di chiunque, comparandoli con una black list.

Premesso che la Commissione si riferiva a misure molto più generali, non c'è dubbio che i risultati sui sistemi appena citati sono e saranno, per molto tempo, di non elevata probabilità positiva.

Ma questo non significa affatto perdere l'efficacia nei controlli di Polizia, almeno se gestiti correttamente.

Infatti, come ricorda la stessa bozza di white paper, l'emergere di un mach di alerting (da non considerare automaticamente positivo) e la successiva valutazione umana della ripresa sul posto (quindi non c'è alcun automatismo), può portare a tre differenti esiti:

- successivo approfondimento della ripresa effettuata e degli spostamenti del soggetto, secondo regole similari al progetto FIRST o altre procedure analoghe;
- intervento sul luogo con una squadra di intervento rapido, solo quando un operatore qualificato ritenga che, in effetti, quel volto rassomiglia fortemente a quello del ricercato;
- valutazione estemporanea, da parte dell'operatore di Polizia, di non rilevanza dell'alert ricevuto dove, per tutelare i diritti dell'interessato, ritengo sarebbe necessario un automatismo (questo sì) di cancellazione del log di allarme (non delle immagini registrate, che resterebbero conservate secondo i normali criteri per una normale videosorveglianza)

Sul primo caso, come già scritto, abbiamo già commentato l'efficacia di questa tecnologia.

Circa il secondo caso (cioè l'intervento sul posto), è l'esito dell'osservazione delle immagini dal sistema di videosorveglianza e non il primo warning del sistema di riconoscimento facciale a fare scattare l'operazione degli organi di Polizia.

Qualora lo si ritenga proprio necessario, va ricordato che la stessa Direttiva 2016/679 sulla protezione dei dati personali per finalità di Polizia, al Considerando 26, richiama l'impiego dei sistemi di videosorveglianza nell'ambito del "law enforcement", quindi è pacifico che le

Forze dell'Ordine abbiano la facoltà di intervenire anche in caso di riconoscimento di un soggetto dalle immagini riprese dalle telecamere.

Ma quanto detto sopra non tiene conto di un altro, essenziale, elemento di utilità del *facial scan*. Infatti, sebbene sia chiaro che possa produrre risultati solo probabilistici e incerti, è invece certa l'efficacia di prevenzione del sistema, che ha la capacità di poter costituire un valido deterrente in tutti i nodi strategici e gli obiettivi sensibili, poiché nessun ricercato può escludere di essere riconosciuto e arrestato, sul momento o grazie alle immagini successive.

Peraltro, il riconoscimento del volto spinge i ricercati ad utilizzare mascheramenti che renderanno sempre più precaria la loro condizione.

Quanto sopra, tenendo presente che non vanno mai scordati i limiti obiettivi di questa tecnologia che, come scrivevo, sono tanti e notevoli.

Come già detto, questo significa che è necessario effettuare una attenta valutazione:

- sui diritti e le libertà delle persone (perché sono evidenti i rischi sulla materia);
- sui costi/benefici, tenuto conto dei mezzi e del personale che può essere impiegato, sì che solo in casi limitati e ben individuati (comunque non rari) il riconoscimento del volto possa risultare effettivamente utile.

5) Le cautele per evitare abusi

Gli abusi e l'utilizzo non equilibrato, nonché rischioso di sistemi di riconoscimento facciale costituiscono un problema reale ed effettivo.

Per questo, come si è detto in premessa, la bozza del white paper sostiene che è necessario tempo per sviluppare una solida metodologia per valutare l'impatto e le possibili misure di gestione dei rischi Per questo, sarebbero necessari 3-5 anni di interruzione nell'utilizzo di questa tecnologia.

Queste affermazioni non sembrano corrette.

Anzitutto, è assolutamente fuori luogo, a fronte del continuo e incessante sviluppo delle tecnologie, pensare che sarà mai raggiunto un punto di arrivo, né si avrà mai la certezza della validità delle procedure di valutazione di impatto.

Al contrario, solo lo sviluppo continuo e incessante di metodiche aggiornate, basate sull'esperienza, quindi sulla base di attività di trattamento in corso, può ridurre i rischi di un utilizzo improprio sotto una soglia accettabile.

Ancora, bisogna, con realismo, pensare al periodo tempo che è stato necessario per varare il GDPR in ambito UE.

Il primo progetto formale è stato presentato nel 2012. (anche se, nei documenti dell'Unione, se ne parlava già da anni). Premesso che l'impiego della biometria è stato regolamentato proprio dal Regolamento europeo (si veda più avanti), nonostante sia trascorso un arco di tempo di almeno 10 anni, non ci sono ancora certezze legali chiare.

Se non si sono raggiunte certezze finora, si crede veramente di poter trovare una soluzione al tema della biometria in tre – cinque anni, a fronte di un buon decennio di sviluppo nelle esperienze precedenti?

Eppure, le cautele per evitare gli abusi sono già presenti nel GDPR, che ha introdotto regole stringenti per i dati particolari in genere (tra i quali rientrano anche quelli biometrici) e anche la facoltà, degli stati membri, di regolamentare, in forma più stringente, proprio questa materia.

Per altro, non solo il Garante italiano, ma anche molte altre autorità europee, hanno varato regole di utilizzo già da tempo.

Ancora, strumenti più stringenti potrebbero essere introdotti da pareri *ad hoc* del Comitato Europeo sulla Protezione dei Dati, composto dai garanti delle nazioni UE, che invece, per ora, non si è pronunciato.

Al riguardo, considerate le forti differenze di opinione manifestatesi da parte delle autorità che compongono il Comitato, viene da chiedersi se le ipotesi di *facial recognition ban*, allo studio della Commissione Europea, non dipendano dalla effettiva necessità che è stata

enunciata, ma dalla presa d'atto di una oggettiva incapacità di decisione, intervento e vigilanza delle istituzioni a tutti i livelli, a partire da quelle comunitarie.

Insomma: la logica della Commissione sarebbe quella della proibizione, al posto di quella di governare la tecnologia, per scarsa capacità dei governi dell'Unione.

Va aggiunto che, a prescindere da complesse problematiche di competenza delle istituzioni europee, in materia di GDPR e Direttiva 2016/680, la decisione di vietare una tecnologia avrebbe l'effetto di violare il principio di neutralità tecnologica al quale si ispira proprio il Regolamento generale sulla protezione dei dati.

Si noti, infine, che anche il CNIL (il Garante francese), ha lanciato un dibattito sull'impiego del riconoscimento del volto (qui) in "era" GDPR, individuandone i limiti, le criticità e i vantaggi, ma non prospettando il divieto di questa tecnologia a prescindere (anzi, in vari passaggi, indicando una certa apertura sul tema).

a) Segue: sempre sulle misure di sicurezza

Per quanto detto sopra non è, né ragionevole, né legittimo, vietare per principio il riconoscimento facciale nelle aree pubbliche.

Quindi, la palla torna nel campo delle misure di tecniche e organizzative da adottare, poichè è certo che solo con l'applicazione di misure idonee a contenere il rischio consentirebbe di svolgere qualsiasi trattamento, inclusa la biometria facciale, con i limiti del caso.

Al riguardo, lo stesso white paper prevede un elenco di ulteriori criteri da tenere in conto, per trattamenti e tecnologie ad alto rischio, che riassumo molto succintamente:

- definire i settori e le applicazioni ad alto rischio;
- procedure di auto individuazione del rischio attraverso valutazioni preliminari svolte sia dagli sviluppatori che dagli utilizzatori;
- ulteriori tipologie di criteri che tengano conto del contesto, ad esempio tenuto conto dei vantaggi derivanti dagli output e dal rischio di discriminazione;
- considerare gli effetti significativi sugli interessati.

6) Gli effetti sull'industria europea dell'eventuale *facial recognition ban*

Sempre la bozza di white paper in esame ammette candidamente che gli Stati Uniti e la Cina sono i maggiori protagonisti in materia di intelligenza artificiale (di riflesso, in materia di biometria).

Eppure, in Europa esistono importanti eccellenze operanti con successo (con tutti i limiti già enunciati), anche nel settore della biometria del volto.

Quali effetti si avrebbero in caso di *facial recognition ban*? Le industrie europee continuerebbero a investire e innovare in un settore bloccato "per legge"?

E' più che facile prevedere che, trascorsi i 3-5 anni di blocco, le competenze europee in questa materia saranno ormai scomparse e il mercato tornerà, ancora di più, appannaggio delle tecnologie americane o cinesi, per non parlare di proposte provenienti da altri mercati rampanti, tra i quali l'India, l'Indonesia, Israele e altre nazioni dove lo sviluppo di sistemi di intelligenza artificiale, applicati al riconoscimento del volto, procede velocemente e senza limitazioni.

Ci chiediamo, quindi: al momento di applicare le "solide metodologie" auspicate dell'Unione, trascorsi 3-5 anni, che tipologie di tecnologie potremmo applicare nell'ambito dell'Unione, se non quelle extra UE?

Al riguardo, pensiamo alla forza economica e commerciale di colossi come Amazon, Google, Apple, Facebook, Huawei, Dahua in tema di riconoscimento facciale. E' evidente che le proposte, anche nel settore di Polizia (a prescindere dal possibile bando delle aziende cinesi), saranno esclusivamente provenienti da soggetti di questa stazza.

7) Conclusioni

Dopo 5 anni di blocco dello sviluppo tecnologico e predisposto un bel set di questionari e regole per la biometria, pensate veramente che avremmo maggiore protezione dei diritti e delle libertà degli interessati?

Se l'Europa vuole fare come gli struzzi lo faccia pure, ma rinunciando a cavalcare la tigre va incontro a una storica sconfitta.

L'Autore: Aldo Agostini, è Responsabile del Dipartimento protezione dei dati personali di A.I.PRO.S.