# Perché l'Europa sta valutando di bandire il riconoscimento facciale

**Author :** Giovanni Villarosa

**Date :** 11 Febbraio 2020

Torniamo a parlarne di **intelligenza artificiale** (AI), della spigolosa questione inerente la sicurezza degli algoritmi e delle tecnologie per il riconoscimento facciale; lo facciamo dopo aver letto la pubblicazione di un nuovo *paper,* secondo il quale Bruxelles sta valutando concretamente l'ipotesi di mettere in *stand-by*, per il prossimo quinquennio, l'impiego dei **sistemi di identificazione artificiale** nei luoghi pubblici dell'intera Unione.

Una logica artificiale che interfaccerà sempre di più l'uomo alla macchina, dove gli algoritmi saranno sempre di più il tramite multiplo (giuridico, tecnologico, etico) del collegamento cyber, perché aggregando, analizzando milioni di dati istantaneamente, profilano comportamenti, prevedono scenari, monetizzano dati, minacciando però, pesantemente, **la nostra libertà** con la loro intelligenza di plastica.

Negli ultimi venti anni la tecnologia è passata da un semplice codice numerico (PIN) ai lettori della geometria della mano, dalla lettura delle impronte digitali alla scansione dell'iride, sino ad arrivare, oggi, alla grande rivoluzione biometrica della geometria del volto.

Un esempio su tutti è rappresentato dalla mappatura dei vasi sanguigni, ricavata da immagini infrarosse (IR), **dati biometrici** utilizzati per estrarre la conformazione geometrica (univoca) dei vasi interni al volto umano; mappe, queste, utilizzate come vere impronte digitali facciali, biologicamente uniche.

Come detto, in queste ultime settimane la Commissione europea si è nuovamente occupata di tecniche e tecnologie applicate nel riconoscimento facciale e lo ha fatto pubblicando un white paper; si tratterebbe di un *ban temporaneo*, ritenuto dai più necessario affinché si possano **valutare i rischi e adottare le adeguate contromisure**, tanto dal punto di vista legislativo quanto da quello tecnologico.

Proprio su questi propositi la Commissione europea avrebbe predisposto un *dossier* dove elenca tutte le criticità fino ad oggi emerse nel riconoscimento facciale, le linee guida da seguire

a prevenzione degli abusi e le istruzioni obbligatorie da dettare agli addetti ai lavori, ma sopratutto ai **cittadini sorvegliati.**

Il documento preannuncia uno specifico quadro regolatorio sull'AI, che potrebbe includere un divieto temporaneo (5-3 anni) sull'utilizzo di tale tecnologia; uno stop temporale all'interno del quale dovrà essere elaborata "*una solida metodologia per valutare gli impatti di questa tecnologia e le possibili misure di gestione del rischio*".

Sul tavolo di lavoro sono state messe in discussione ben **cinque opzioni possibili**, da approvare, presumibilmente, entro il mese di febbraio 2020.

In una prima ipotesi si parla di una generica *compliance*, ma esclusivamente su base volontaria: tutti gli sviluppatori potranno scegliere se aderire a determinate norme sulla cd. **intelligenza etica**, ottenendo così una sorta di bollino che garantirà (o certificherà?), rispettando precisi requisiti, affidabilità e sicurezza del prodotto.

Altra ipotesi è quella di optare a **requisiti specifici**, vincolandoli alla sola pubblica amministrazione, adottando una sorta di *directive on automated decision making*, tenendo in debita considerazione il vincolo del Regolamento GDPR sul diritto a non essere soggetti a una decisione basata esclusivamente sull'elaborazione automatizzata, inclusa la profilazione.

Una terza opzione si fonda sui requisiti obbligatori impostati sui livelli di rischio, delineando quei settori cd *sensibili*, individuati nelle aree sanità, trasporti, autorità di polizia e giudiziaria, ovvero, là dove sia possibile causare un danno fisico o materiale all'interessato.

Una quarta opzione è relativa alla tematica della *governance*; a questo proposito si fa strada la creazione di un efficiente sistema di attuazione e controllo delle regole, mediante supervisione pubblica, coinvolgendo le singole autorità nazionali.

Altro (e ultimo) importante aspetto oggetto di analisi è relativo alla **sicurezza** e alla **responsabilità**, perché su questi due delicati temi potrebbero essere necessari specifici adeguamenti regolatori, per meglio definire le responsabilità che ricadrebbero sugli sviluppatori, distinguendola da quella dei produttori.

Sappiamo bene come l'uso del riconoscimento facciale stia crescendo in maniera esponenziale; e non solo per finalità legate alla sicurezza ma in ambiti sempre più disparati, come ad esempio nei centri commerciali, per profilarne la clientela.

Una tecnica biometrica idonea ad identificare in modo inequivocabile un individuo, confrontando e analizzando modelli matematici, basata sulla sua geometria del volto, come ad esempio il riconoscimento facciale generalizzato o quello adattativo, evolvendo sempre di più verso **nuovi approcci a tecnologia 3D**, una tecnica decisamente più pervasiva.

Abbiamo visto brevemente come lo stato dell'arte per il riconoscimento facciale permetta di raccogliere informazioni sulle caratteristiche biometriche di una persona, classificandole sotto forma di **dati personali sensibili**.

In questa fattispecie una barriera normativa a garanzia del trattamento indiscriminato dei dati personali trattati con mezzi elettronici, è rappresentata dai diversi articoli e considerando, contenuti nel Regolamento europeo aggiornato GDPR UE 2016/679:

## Art. 4

*1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)…*

*2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati…*

*4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati… in particolare per analizzare… la salute… l'ubicazione o gli spostamenti di detta persona fisica…*

*14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche… quali l'immagine facciale…*

## Art. 9

*1) è vietato trattare dati personali che rivelino l'origine razziale o etnica… nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica…*

Ora, alla luce di quanto considerato è indubbio il fatto, come, per trattare legittimamente i dati di natura biometrica (nel vecchio codice privacy erano considerati come **supersensibili**), sia obbligatorio utilizzare le basi giuridiche rinvenute nell'art. 9 punto 2, in particolare quella contenuta nella lettera a):
"*l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1".*

Appare chiaro come il **consenso dell'interessato** rappresenti uno dei punti nodali per la necessaria *compliance* al GDPR, perché questa non deve soddisfare solamente i requisiti previsti nell'art. 9, ovvero l'esplicito consenso, ma anche da quanto prescritto per le condizioni del consenso all'art. 7, ancor meglio al punto 1):

*qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.*

Orbene, quanto detto trova ulteriore sostegno nelle Linee Guida WP259, dove al punto 4 il consenso esplicito è richiesto in quelle particolari circostanze - e il riconoscimento facciale è tra queste - dove emergano gravi rischi.

Tuttavia, oltre al consenso diretto dell'interessato, vanno considerati altri aspetti fondamentali

quando trattiamo dati di natura biometrica: la protezione dei dati fin dalla fase di progettazione (*privacy by design* e *by default*, art. 25), la valutazione di impatto (DPIA, art. 35), la consultazione preventiva con l'Autorità Garante (art. 36) quando l'attività di valutazione di impatto presenta un **rischio elevato** nel trattamento dei dati (esempio la videosorveglianza su larga scala).

Invero, secondo le Linee Guida WP248, per determinare se un trattamento avviene su larga scala si dovrà fare riferimento a:

- al numero degli interessati;
- al volume dei dati;
- alla tipologia dei dati;
- alla durata dell'attività di trattamento;
- all'ambito geografico dell'attività di trattamento.

Andranno poi valutate tutte le adeguate **misure di sicurezza** rapportate al rischio del trattamento per garantire la protezione dei dati, dimostrandone la conformità al GDPR che richiede misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 32), tenendo sempre conto dei diritti e degli interessi legittimi degli interessati.

Dunque, sarà sempre opportuno ponderare un efficiente sistema di *Data Loss Prevention* (per fronteggiare eventuali ipotesi di *data loss* e *data leak)*, un robusto piano di *Disaster Recovery*, come un'efficace policy di *backup* dei dati, conforme al Regolamento.
Perciò: sono sufficienti, allo stato dell'arte, le attuali misure di sicurezza logica, le cd. misure *cybercrime,* applicabile alla *face recognition*?

Per chiudere, **due esempi** di scuola. Nel 2018 la polizia di Stato australiana testò un software di riconoscimento facciale connesso a un sistema di videosorveglianza pubblica, indirizzato all'identificazione di alcuni *target high profile*; ebbene, il sistema è stato in grado di identificare solamente 5 delle 268 persone sorvegliate, un **clamoroso flop** che spinse ancor di più l'*Australian Human Rights Commission* (AHRC, agenzia governativa), a confermare l'inaffidabilità di questa tecnologia, insicura anche dal punto di vista degli attacchi hacker.

In **Francia**, timori geograficamente opposti, ma simultaneamente identici: lo scorso anno un hacker impiegava poco più di un'ora per bucare una App istituzionale (con identificazione facciale) in uso alla messaggistica governativa, definita inviolabile.

Che dire? Ho letto decine di testi sull'argomento, partecipato a numerosi corsi universitari di alta formazione (*video analysis, facial recognition, cyber awareness, critical thinking*) sull'uso della AI e IoT nel campo della *Security,* ma sempre mi torna in mente questa frase: "*la sicurezza informatica sarà sempre una chimera finché esisterà il fattore umano, l'anello più debole della catena della sicurezza".*
Una massima tratta dal libro "L'arte dell'inganno*",* saggio scritto da **Kevin Mitnick** (Feltrinelli), considerato dal *bureau* statunitense (FBI) il *miglior e più abile* Hacker del mondo, il massimo esperto di tecniche di *social engineering;* Mitnick nel testo ci spiega come tutti i possibili e superiori algoritmi possono essere messi fuori uso, in discussione, da semplici pratiche

di **ingegneria sociale**, capaci di catturare dati personali con una banalissima telefonata, a totale insaputa degli interessati, superando tutti i più robusti livelli di sicurezza logica - la cd. *cybersecurity* - in una maniera tanto "rustica" quanto disarmante.

Articolo a cura di **Giovanni Villarosa**