PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4890 di Venerdì 12 marzo 2021

Le linee guida europee sugli applicativi di riconoscimento facciale

Le perplessità sugli utilizzi di algoritmi di riconoscimento facciale, sia dal punto di vista di validità tecnica che del trattamento di dati personali sono numerosissime. Un documento offre linee guida tanto autorevoli, quanto incisive.

Punto Sicuro più volte ha trattato questo argomento, mettendo in evidenza problemi sia di natura tecnica, sia di natura legislativa, connessi all'utilizzo degli algoritmi di riconoscimento facciale. Ad esempio, negli Stati Uniti è stato appurato il fatto che questi algoritmi sono assai poco efficaci nel riconoscere determinate categorie di persone; in Europa, i difensori della protezione dei dati hanno avanzato numerose perplessità in merito alle modalità con cui questi applicativi vengono installati ed utilizzati.

Non per nulla, la Convenzione per la protezione degli interessati in fase di trattamento di dati personali, chiamata Convenzione 108+, all'articolo 6 specificamente include questi dati fra le speciali categorie di dati, che devono essere trattati con particolari cautele. Ecco il motivo per cui chiunque voglia utilizzare questi applicativi deve leggere con attenzione non solo il regolamento generale sulla protezione dati personali, ma anche questa Convenzione.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0551] ?#>

La crescente diffusione di sistemi di videosorveglianza rappresenta un problema, quando gli applicativi di riconoscimento facciale sono integrati in questi impianti. Ecco perché, anche laddove sia possibile installare impianti di videosorveglianza, occorre fare attenzione a come i dati ripresi vengono trattati: sotto certi aspetti, il problema non è molto diverso da quello che si pone quando vengono installati gli applicativi di video control Analysis.

Un ulteriore aspetto che occorre esaminare riguarda il fatto che questi impianti vengono gestiti da pubbliche autorità, rispetto a quelli gestiti da enti privati. È evidente che le finalità delle pubbliche autorità possono essere diverse, i più estese, rispetto a quelle di un ente privato.

Quando si decide di installare un applicativo di riconoscimento facciale, il Consiglio d'Europa suggerisce di prendere in esame i seguenti aspetti:

- sviluppare una dettagliata analisi delle finalità e degli obiettivi dell'applicativo,
- offrire alcune indicazioni sulla affidabilità e l'accuratezza dell'algoritmo utilizzato,
- indicate il periodo di archiviazione delle immagini,
- introdurre criteri per effettuare degli audit di conformità dei parametri precedenti,
- consentire la tracciabilità dell'intero trattamento,
- indicare quali salvaguardie verranno utilizzate.

La faccenda diventa ancora più complicata se l'applicativo di riconoscimento facciale archivia i volti catturati in un data base, per futuri riconoscimenti automatizzati. Anche in questo caso, le linee guida differenziano i comportamenti da tenere a seconda del profilo del titolare del trattamento.

Nell'ambito privato, le tecniche di riconoscimento facciale possono essere utilizzate solo se il soggetto ripreso da un libero consenso; ciò significa che, ove il riconoscimento facciale venga utilizzato per sistemi di controllo accesso, occorre mettere a punto strumenti alternativi di controllo, se il consenso non viene rilasciato.

Da questo punto di vista, la soluzione non è molto diversa rispetto a quella già in vigore per altri tipi di riconoscimento biometrico.

Le linee guida passano poi ad analizzare la qualità degli algoritmi utilizzati.

Come accennato in precedenza, su questo tema sono numerose le perplessità ed occorre quindi che la software house, che ha sviluppato l'algoritmo, dimostri come ha potuto correttamente riconoscere immagini di uomini, donne, con diversi colori della pelle, diversa morfologia, diversa età e con riprese effettuate da angolazioni diverse.

Poiché una possibile violazione dei dati può avere un impatto significativo sugli interessati ripresi, i titolari del trattamento dovranno adottare misure particolarmente incisive di protezione dei dati, garantendo la protezione da attacchi fisici ed attacchi informatici.

Tutti i soggetti coinvolti nel trattamento di dati personali devono essere specificamente addestrati e dotati di strumenti, che possono mettere tempestivamente sotto controllo potenziali anomalie.

Questa precisazione ovviamente vale per titolari pubblici e privati.

Deve essere sviluppato, come attività obbligatoria per ogni trattamento, una valutazione di protezione dei dati in conformità all'articolo 25.

Non v'è dubbio che, data la criticità del trattamento, si debba sviluppare anche una valutazione di impatto, in conformità all'articolo 35 del regolamento generale europeo; tale documento, per evidenti ragioni, deve essere periodicamente riesaminato ed aggiornato.

Infine, è indispensabile prendere in considerazione gli aspetti etici, afferenti all'utilizzo di queste tecnologie, in quanto è evidente che potrebbero crearsi delle situazioni estremamente delicate, ove il volto di un soggetto ripreso venga abbinato a movimenti o spostamenti, effettuati in contesti altrettanto delicati (si pensi alla ripresa di un soggetto che interagisce con una prostituta sulla pubblica via!).

Infine, il documento mette in evidenza i diritti degli interessati ripresi, soprattutto in riferimento alla esigenza di correggere abbinamenti effettuati con database automatizzati, che possano ripetersi più di una volta. In questo caso è evidente che l'anomalia riguarda l'affidabilità dell'applicativo e occorre quindi provvedere alla correzione di questi abbinamenti automatici. Ecco la ragione per la quale ogni abbinamento automatico deve comunque essere convalidato da un operatore umano.

Tutti gli specialisti di protezione dei dati non possono che ringraziare il Consiglio d'Europa per aver messo a disposizione questo prezioso documento, la cui validità è evidentemente estesa a tutti paesi europei.

Vedi allegato (pdf)

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

---

www.puntosicuro.it