PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5176 di Mercoledì 01 giugno 2022

Attenzione all'utilizzo improprio di applicativi di riconoscimento facciale

Il comitato europeo per la protezione dei dati ha pubblicato un documento che vuole aiutare le forze dell'ordine ad utilizzare questi preziosi applicativi, senza tuttavia violare precise disposizioni europee, come il patto europeo sui diritti fondamentali

Ormai è una procedura standard, che le forze dell'ordine, coinvolte nelle indagini afferenti, ad esempio, ad un incidente stradale od una rapina, di recuperare tutte le registrazioni delle videosorveglianza delle telecamere, che possono aver coperta la zona dove si è verificato l'evento, ed analizzare le singole immagini, per individuare i volti dei soggetti coinvolti, ad esempio rapinatori.

A questo fine, si utilizzano degli applicativi di intelligenza artificiale, che permettono di analizzare rapidamente un gran numero di dati. Questi applicativi vanno sotto la generica classificazione di tecnologie di riconoscimento facciale (FRT-facial Recognition technology).

Questi applicativi evidentemente trattano dati biometrici e come tali devono essere utilizzati in contesti strettamente controllati. Ad oggi purtroppo non sono disponibili specifiche disposizioni legislative che possono permettere di dare applicazione pratica dei principi generali illustrati nel già menzionato patto europeo sui diritti fondamentali.

In attesa della pubblicazione di specifiche disposizioni legislative, questo documento vuole offrire una linea guida a tutte le forze dell'ordine, nonché le procure della Repubblica, per un utilizzo appropriato di questi applicativi FRT.

Ad esempio, non è possibile utilizzarli senza avere sviluppato una valutazione di impatto, secondo l'articolo 35 del regolamento generale europeo; l'esperienza mostra come molto spesso i soggetti coinvolti non provvedono a questo fondamentale valutazione. Occorre inoltre garantire un elevatissimo livello di sicurezza, nel trattamento di questi dati, per le ovvie conseguenze di una possibile violazione dei dati, anche di natura accidentale.

Occorre introdurre delle rigide regole che definiscono il profilo degli autorizzati ad accedere a questi applicativi, in modo che il principio di minimizzazione di accesso ai dati e degli operatori autorizzati sia sempre rispettato.

Per meglio chiarire alcuni aspetti applicativi di queste linee guida, il documento illustra sei ben diversi realistici, scenari, che aiutano a meglio comprendere se come e quando è possibile utilizzare applicativi di intelligenza artificiale nel contesto di indagini su reati.

Ecco l'illustrazione di un primo scenario.

Ci troviamo al punto di controllo passaporti di un aeroporto europeo. È attivo un sistema di lettura automatica del passaporto e di cattura, mediante telecamera, del volto del passeggero. L'applicativo effettua un controllo incrociato tra la fotografia riportata sul passaporto e l'immagine catturata. Se vi è ragionevole congruità fra queste due immagini, il tornello si sblocca e il passeggero può attraversare il punto di controllo.

La faccenda diventa più interessante quando, con l'occasione di questo controllo, si invia la foto acquisita ad un sistema di intelligenza artificiale, collegato ad un database di soggetti sottoposti a specifiche limitazioni di accesso e transito nell'unione europea.

In questo caso, viene effettuato solo un confronto locale fra due immagini, ma viene attivata una procedura, che potrebbe portare addirittura all'arresto del passeggero, se l'intelligenza artificiale rilevasse una ragionevole congruità tra l'immagine catturata e l'immagine archiviata nel database di soggetti pericolosi. A questo punto occorre sviluppare un processo di valutazione di necessità e proporzionalità del trattamento, che porta indubbiamente a ritenere che le esigenze di sicurezza della unione europea debbano e possano essere tutelate anche con questo specifico trattamento.

Si giunge infine alla conclusione che la verifica dell'identità di un cittadino europeo, nel contesto di un sistema automatico di controllo dei passaporti, rappresenti una misura proporzionata e necessaria, a condizione che vengano attivate adeguate misure di trasparenza dell'operazione e sia garantito elevato livello di sicurezza dell'operazione stessa.

Vedi allegato (pdf)

Adalberto Biasiotti