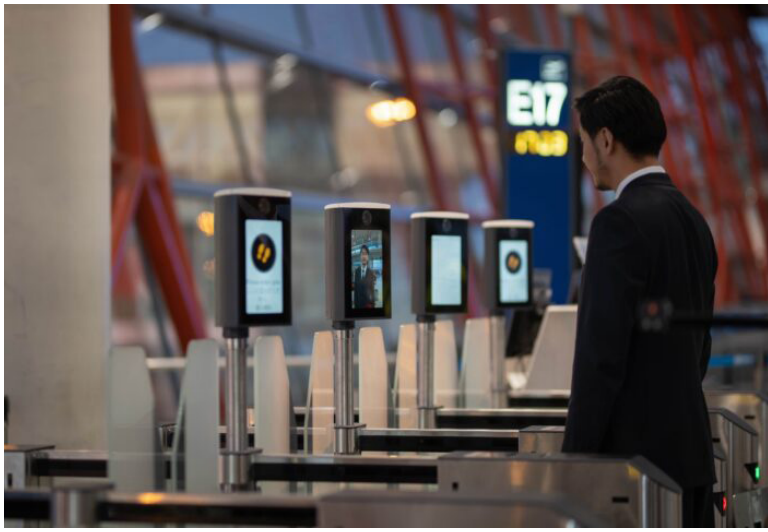
Dove finiscono i dati del FaceBoarding in aeroporto? Tutte le domande e i rischi per la privacy

Vi ricordate di *Minority Report*? Mi riferisco al film di **Steven Spielberg**, datato 2002 e liberamente tratto dall'omonimo racconto di fantascienza di **Philip K. Dick**, *Rapporto di minoranza*. Nella pellicola veniva riprodotta la realtà distopica di una Washington proiettata nel 2054, dove una diffusa rete di telecamere veniva utilizzata per identificare costantemente la popolazione e, incrociando quei dati con un sistema predittivo, si potevano arrestare i soggetti prima che questi compissero gli atti criminosi, in base al giudizio prognostico di questo sistema.

Scenario inquietante e possibile, ma che sembrava lontano dal potersi concretizzare nelle realtà occidentali, mentre in **Cina** è già da tempo sostanzialmente vicino dal pieno compimento.



In realtà, anche in Occidente i **pruriti tecnologici** piano piano superano ogni ostacolo prima culturale e poi normativo, e se negli Stati Uniti, ad esempio, il **FaceBoarding** è già attivo in diversi aeroporti, in Europa l'Italia per prima ha voluto varcare la frontiera del **riconoscimento biometrico facciale** per facilitare i requisiti di accesso ai gate di imbarco. Infatti, il 7 maggio è stato inaugurato all'**aeroporto di Linate** un nuovo sistema di questo tipo che, come assicurato da Sea S.p.A., società che gestisce gli aeroporti milanesi, **"garantisce la tutela della Privacy e dei dati dei passeggeri"** per mezzo di una "tecnologia sicura, semplice e rapida".

Tecnicamente, il riconoscimento facciale è basato sulla raccolta ed elaborazione delle caratteristiche biometriche del volto, dalle quali vengono estratti un certo numero di tratti biometrici, come la posizione, la distanza e la misura degli elementi che connotano il volto, al fine di costruire un **modello biometrico**, ossia un insieme di tratti biometrici memorizzati in forma digitale.

Dal punto di vista giuridico, ognuno di questi elementi rientra nella definizione di dato biometrico, che il **Regolamento (UE) 679/2016** (General Data Protection Regulation – **GDPR**) annovera nell'ambito delle categorie particolari di **dati personali** (i cosiddetti "dati sensibili"), il cui trattamento è soggetto a una disciplina più rigorosa, in considerazione dei rischi che possono derivare per i diritti e le libertà delle persone.

Quali potrebbero essere questi rischi? Alcuni sono facilmente immaginabili, come il furto di identità e il conseguente utilizzo dei dati biometrici per la realizzazione di azioni fraudolente. Per questo, il trattamento dei dati biometrici richiede l'adozione di **misure di sicurezza** particolarmente elevate, sulle quali gli interessati hanno il diritto di essere informati. E anche l'informativa sul trattamento dei dati personali attraverso il servizio di FaceBoarding, presente sul sito web dell'aeroporto di Linate, fornisce alcune indicazioni in tal senso, specificando che i dati biometrici sono **conservati**, sotto forma di modello biometrico, in **forma crittografata**.

Informazioni un po' scarne, in effetti. Ci si potrebbe domandare, ad esempio, quale sia l'algoritmo utilizzato per cifrare i modelli biometrici, quali siano i livelli di autorizzazione applicati per l'accesso al **database** che

li ospita, in che modo viene protetta la trasmissione dei dati biometrici acquisiti tramite i chioschi presenti in aeroporto verso i sistemi informatici aeroportuali.

A partire da giugno, inoltre, i dati biometrici associati al volto dei passeggeri potranno essere acquisiti tramite "**selfie**" in caso di registrazione via App. Anche in questo caso, dall'informativa non emergono altri dettagli sul processo di acquisizione dei dati biometrici tramite App, che potrebbe comportare ulteriori rischi, non di poco conto.

È noto, infatti, che le caratteristiche biometriche del volto possono essere ricavate anche da **immagini fotografiche**, che oggi, con l'impiego di sistemi di intelligenza artificiale ormai accessibili e facilmente utilizzabili da chiunque, possono essere rielaborate in modo da ottenere una ricostruzione del volto molto fedele a quella di una persona in carne ed ossa (ad esempio, mediante la realizzazione di modelli tridimensionali) in grado di ingannare i sistemi di acquisizione tramite **smartphone**.

Tanto più, in assenza di qualsiasi controllo umano, dal momento che, come si legge nell'informativa, la "scelta di effettuare le operazioni di identificazione tramite biometria comporta che la verifica della Sua identità avverrà in maniera interamente automatizzata".

In effetti, tutti i rischi che potrebbero derivare dall'uso di questo sistema di FaceBoarding, comprese le scelte relative a tempi stabiliti per la conservazione di questi dati, dovrebbero essere stati attentamente verificati e documentati all'interno di una valutazione d'impatto sulla protezione dei dati, che il GDPR impone di effettuare in caso di trattamenti particolarmente delicati e impattanti sui diritti fondamentali delle persone coinvolte in tali trattamenti. Ma questo non si evince dalla lettura della striminzita informativa fornita.

In estrema sintesi, il problema non è la tecnologia utilizzata, ma **l'attenzione alla protezione dei dati trattati** tramite determinati sistemi e – per quelli più invasivi – la trasparenza non dovrebbe mai essere "striminzita", ma dovrebbe sempre consentire di verificare che siano stati coniugati sapientemente i diritti degli interessati – correttamente informati (anche ai fini dell'acquisizione di un valido consenso)– con le esigenze di efficientamento degli ingressi ai gate, abbinate a ragioni di sicurezza.

D'altra parte, non si possono trascurare i diritti fondamentali e la predisposizione di misure di scurezza adeguate a evitare questi rischi gravissimi per i passeggeri, magari confidando in una sorta di "**assuefazione alla privacy**" che pericolosamente caratterizza gli ultimi tempi digitali che stiamo vivendo.

Insomma, l'Europa (e probabilmente gli Usa) sono attualmente lontani dall'utilizzare tecniche di *social scoring* e di giustizia predittiva come paventati da certi futuri distopici ipotizzati in alcuni film di fantascienza, ma l'attenzione al tema deve essere sempre massima e la trasparenza informativa, se sviluppata in modo efficace (magari sostenuta da politiche di alfabetizzazione su questi temi) potrebbe favorire una c**onsapevolezza diffusa** della cittadinanza digitale.

E ricordiamoci che è proprio la consapevolezza **l'unica arma disponibile** che possa allontanare certi scenari distopici dai nostri orizzonti di vita realmente digitale.

9 Maggio 2024

Andrea Lisi
Avvocato, esperto in diritto dell'informatica, Presidente di ANORC Professioni.

Articolo scritto per il suo Blog ospitato su Il fatto quotidiano: https://www.ilfattoquotidiano.it/2024/05/09/dove-finiscono-i-dati-del-faceboarding-in-aeroporto-tutte-le-domande-e-i-rischi-per-la-privacy/7542329/