Digeat N.2 - 19 Giugno 2024

L’autenticazione biometrica: tra Amazon One, Faceboarding e i divieti imposti dall’AI Act

Di Federica Marchi

Abstract

Lo sviluppo tecnologico ha determinato innovazioni che non si sono limitate a creare una diversa ed autonoma “realtà” virtuale, ma che hanno influito sensibilmente su quella effettiva, modificando i rapporti umani ed economici e lo stesso modo di intendere il sistema ordinamentale. In questo senso, l’utilizzo dei dati biometrici non rappresenta una novità: se in alcuni Stati costituiscono uno strumento nelle mani del governo e delle forze dell’ordine, negli ultimi anni il loro utilizzo da parte di produttori di beni di consumo a scopo di autenticazione è aumentato vertiginosamente. L’autenticazione biometrica per accedere ai nostri device personali, infatti, costituisce un’alternativa sempre più diffusa all’utilizzo di password: è più semplice, più veloce e – teoricamente – più sicura. Tuttavia, l’uso della biometria comporta rilevanti implicazioni etiche e legali, soprattutto in termini di privacy e sicurezza in rete, che meritano di essere analizzate anche alla luce della disciplina introdotta dall’AI Act.

Indice

I dati biometrici: cosa sono e come funzionano

Ai sensi dell’art. 4, par. 1, n. 14 del Regolamento UE 2016/679 (c.d. GDPR), i dati biometrici sono i “*dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloscopici*”.

Questi, rientrano tra le categorie di dati personali soggetti alla speciale tutela normativa ex art. 9 GDPR rappresentando, in altre parole, quei “tratti distintivi” fisici o comportamentali che ci rendono chi siamo e che possono essere utilizzati per identificarci o autenticarci in maniera univoca.

In questo senso, però, già nel 2007 il Working Party sull’art. 29[1] operava una distinzione **tra il dato biometrico vero e proprio** – ovvero, il dato trattato che identifica direttamente una persona quale, per esempio, l’impronta del viso o il suono della voce – **e la fonte da cui questo viene semplicemente estratto** – che può essere rappresentata, rispettivamente, da una fotografia o da una registrazione

audio – dal momento che, entrambe, possono costituire oggetto di un trattamento volto a rilevare le caratteristiche proprie di una persona. **La differenza tra queste due nozioni risiede nelle modalità di rilevazione e nella finalità perseguita tramite detto trattamento**: affinché si possa parlare di trattamento di dati biometrici ai sensi del GDPR e, dunque, soggetto alle eccezioni di cui all'art. 9 cit., sarà necessario che "*i confronti finalizzati al riconoscimento dell'individuo (verifica dell'identità, nel caso in esame) siano automatizzati mediante l'ausilio di appositi strumenti software o hardware*"[2]. Appare, dunque, lecito affermare che, qualora la finalità del trattamento non sia quella di identificare univocamente un individuo, i dati rilevati senza l'utilizzo di un dispositivo tecnico dovranno essere tutelati come normali dati personali[3].

Ad ogni modo, in base alla definizione normativa fornita dal GDPR, **si è soliti distinguere l'autenticazione biometrica in "biometria fisiologica"** – come, ad esempio, le impronte digitali e la scansione del volto, generalmente utilizzati per sbloccare lo *smartphone* in alternativa al tradizionale PIN – che si caratterizza per il rilevamento automatizzato di caratteristiche fisiche che consentono l'identificazione della persona, **e in "biometria comportamentale"** – quali il riconoscimento vocale e la firma grafometrica, utilizzati anche nei servizi bancari – che consente unicamente di valutare la riferibilità dei dati rilevati a una persona di cui siano stati precedentemente acquisiti e registrati.

In entrambi i casi, i sistemi di riconoscimento biometrico funzionano in due fasi: l'acquisizione e l'estrazione-confronto. Infatti, una volta che i dati biometrici vengono acquisiti mediante un sensore, le caratteristiche del dato raccolto tramite detta componente *hardware* vengono, poi, estratti da un *software* e, quindi, confrontati con un *database* di modelli predefiniti al fine di autenticare o identificare l'interessato.

> Come detto, i risultati di un simile rilevamento, a prescindere che si tratti di una caratteristica fisica o comportamentale dell'individuo, sono classificati come "dati particolari" soggetti al trattamento speciale di cui al citato art. 9. Di conseguenza, il loro trattamento è vietato, a meno che non si rientri nelle specifiche esenzioni di cui al par. 2 del medesimo articolo, prima fra tutte il consenso dell'interessato che deve sempre essere specifico, informato, libero ed esplicito.

La particolare natura di tali dati, comunque, fa sì che si ponga l'attenzione non solo sulla base giuridica prescelta per il loro trattamento, ma anche al principio della *privacy-by-design* e allo svolgimento di una specifica valutazione d'impatto ai sensi dell'art. 35 del GDPR, tenendo sempre conto, dunque, dei principi di necessità e proporzionalità del trattamento[4].

Pro e contro della biometria

I vantaggi che derivano in termini di comodità ed efficienza dal riconoscimento delle persone mediante il ricorso al dato biometrico sono innegabili: i processi di identificazione ed autenticazione, infatti, **possono essere automatizzati ed eseguiti in modo continuo, senza interrompere l'esperienza degli utenti durante l'erogazione del servizio, divenendo così più rapidi, semplici ed intuitivi**.

Tuttavia, se per un verso l'utilizzo della biometria risulta essere incoraggiato in luogo della più tradizionale *password* poiché, essendo dati – teoricamente – difficili da falsificare o rubare, offrono un maggior livello di sicurezza, dall'altro risulta altrettanto necessaria la predisposizione di specifiche cautele, volte a dirimere tutti i rischi e i pregiudizi per l'interessato, anche connessi alla fruizione non autorizzata di tali dati al di fuori delle finalità originariamente previste.

Più precisamente, i sistemi di riconoscimento biometrico, trattandosi di sistemi automatizzati basati sia su una grande quantità di dati previamente raccolti – **contraddicendo il generale principio di minimizzazione dei dati** – sia su algoritmi i quali devono essere adattati ai cambiamenti delle caratteristiche fisiche e comportamentali degli utenti, possono essere soggetti a **errori, false corrispondenze e, infine, discriminazioni** basate non solo su razza, sesso ed etnia, ma anche su

altri fattori quali, tra gli altri, le condizioni atmosferiche e la luminosità in cui avviene la rilevazione.

> Così opinando, è bene evidenziare un concetto: sebbene sottrarre l'impronta digitale non sia semplice come rubare una carta di credito, anche i dati biometrici, al pari degli altri dati personali, possono essere rubati e utilizzati in modo dannoso per gli interessati. Anzi, vi è di più. Il danno causato dal furto di un dato biometrico, consistendo in un sistema di autenticazione univoco dell'individuo, può determinare conseguenze notevoli per l'intera vita dell'interessato, dal momento che questi dovrà presumibilmente convivere con quella specifica impronta del volto o delle dita per sempre.

In un'epoca caratterizzata da sempre più frequenti Data Breaches, che dimostrano, di volta in volta, come sia sempre più difficile garantire una protezione dei dati personali adeguata, si può affermare che la raccolta e l'archiviazione dei dati biometrici sollevi inevitabilmente delle questioni in termini di protezione e sicurezza degli stessi.

L'approccio europeo *v.s.* extra-europeo: un confronto

Il 20 dicembre 2021, l'*European Data Protection Board* ha pubblicato **un'analisi approfondita circa i rischi e i benefici connessi all'uso dell'autenticazione biometrica in ambito privacy all'interno del TechSonar 2021-2022**.

Il tenore del Report, teso ad **incoraggiare l'uso di tali tecnologie** tenendo comunque alta l'attenzione sulle implicazioni etiche e legali che ne derivano, si pone in linea con l'approccio dimostrato negli ultimi tempi dal legislatore europeo in materia di innovazione, sempre a metà tra l'esigenza di promuovere lo sviluppo tecnologico e garantire al contempo la tutela dei valori costituzionali europei.

Infatti, se al di fuori dei confini UE vi sono Paesi che – in un certo senso – **abusano di tecnologie di IA "ad alto rischio"** quali i sistemi di *Social scoring* o sorveglianza di massa in tempo reale, in Europa non sono mancate sanzioni irrogate dalle autorità garanti nazionali che hanno **valutato caso per caso l'opportunità e l'impatto** di ricorrere a detti strumenti in relazione ai generali principi di necessità, proporzionalità, trasparenza e minimizzazione del trattamento[5], oltre che preoccupandosi di sfatare le ideologie e le inesattezze collegate all'utilizzo di un simile tipo di autenticazione[6].

Il caso Amazon One

Nel 2020, mentre in Olanda l'Autorità garante emetteva un avvertimento formale nei confronti di un supermercato per l'utilizzo ritenuto illegittimo del riconoscimento facciale di clienti e personale al solo fine di prevenire furti e taccheggi[7], negli Stati Uniti Amazon avviava **la sperimentazione del sistema di pagamento *contactless* Amazon One**[8] all'interno dei suoi punti vendita Whole Foods, promettendo di semplificare e migliorare l'esperienza d'acquisto del cliente.

In particolare, la tecnologia Amazon One sfrutta la **scansione biometrica della mano**, attraverso telecamere ad alta risoluzione in grado di acquisire dati quali la sua forma, le vene sottocutanee e tutte le altre caratteristiche distintive, per creare una rappresentazione numerica vettoriale unica del cliente, la c.d. "firma del palmo".

> La scelta di procedere all'autenticazione tramite il riconoscimento del palmo non è casuale. Questo sistema "senza contatto", oltre a soddisfare le esigenze connesse al periodo del Covid-19 in termini di praticità ed igiene, viene considerato meno invasivo – non essendo possibile identificare un individuo sulla base della sola immagine della sua mano – lasciando, inoltre, all'utente il pieno controllo circa il momento e il luogo in

> cui usufruire del servizio e risultando, quindi, *compliant* in tema di consenso esplicito dell'interessato.

Così, previa registrazione in *app* o in *store* inserendo solamente un'immagine della mano da associare alla carta di credito/debito e al numero di telefono, ai consumatori **basta posizionare per qualche secondo il palmo della propria mano sul lettore ottico per finalizzare il pagamento**, senza il bisogno di ricorrere al portafoglio o al *wallet* sullo *smartphone*.

Una volta raccolti, i dati biometrici dell'utente vengono crittografati e associati al suo *account* Amazon, rimanendo memorizzati e conservati in una "zona altamente sicura", separata dagli altri dati dei consumatori, dei server AWS appositamente realizzata per Amazon One.

Tale modalità di trasmissione e successivo stoccaggio costituisce il fulcro delle *privacy* e *security policies* attuate dal colosso dell'*ecommerce*: **evitando che i dati biometrici acquisiti rimangano salvati sul dispositivo Amazon One e disponendo che vengano archiviati in *cloud* più sicuri e isolati**, si andrebbe così a garantire la riservatezza e il controllo degli accessi, che resta consentito unicamente ai soggetti a ciò autorizzati.

Tuttavia, **simili premure non sono bastate ad eliminare le preoccupazioni degli esperti privacy** poiché Amazon, avendo stretto accordi con le principali banche USA per consentire il corretto funzionamento del suo servizio, avrebbe astrattamente la possibilità di combinare i dati biometrici, gli account Amazon e le informazioni sulle carte dei consumatori e, di conseguenza, disporrebbe di **uno strumento potenzialmente idoneo a tracciare le scelte dei suoi utenti,** nonché a fornire nel tempo annunci, offerte e consigli targettizzati sui loro specifici interessi.

Sul punto, non sono mancate le rassicurazioni da parte del gigante *tech* il quale, dapprima, ha riferito che il dispositivo Amazon One non tiene traccia "di ciò che si fa o si acquista" – in quanto questi dati non vengono associati all'identità biometrica – e, successivamente, ha confermato sia di non condividere i dati palmari con soggetti terzi sia di non usarli per scopi di marketing o per qualsiasi altro motivo.

Nonostante ciò, però, **nel 2021 i senatori Amy Klobuchar, Bill Cassidy e Jon Ossoff inviavano una lettera aperta al CEO, Andy Jassy, sollecitando chiarimenti sui progetti di espansione dell'utilizzo di tale tecnologia e palesando le loro perplessità in tema di conservazione e riservatezza dei dati**, mentre **nel 2023 veniva pubblicata la proposta di *class action* Rodriguez Perez v. Amazon.com, Inc.** – terminata pochi mesi dopo con ***notice of voluntary dismissal* in ossequio alla legge federale** – presso il Tribunale distrettuale degli Stati Uniti nel distretto meridionale di New York che eccepiva la mancanza di un'informativa adeguata ai sensi della *Biometric Identifier Information Law* relativamente all'utilizzo dei lettori Amazon One all'interno dei negozi Amazon Go.

Ad ogni modo, ferme queste preoccupazioni, Amazon attualmente **continua a portare avanti i propri progetti di diffusione della sua tecnologia**, concludendo accordi volti ad estenderla a terze parti.

L'uso responsabile della biometria alla luce dell'AI Act

A fronte della recentissima approvazione dell'AI Act da parte del Consiglio europeo, per avere un'idea più chiara di ciò che sarà possibile fare o meno con/dei sistemi di autenticazione biometrica sarà probabilmente necessario attendere la sua effettiva entrata in vigore e, quindi, almeno altri 24 mesi. Questo, infatti, riserva un'attenzione particolare al trattamento dei dati biometrici, classificando i sistemi di identificazione che ne fanno uso tra le tecnologie ad alto rischio idonee a determinare, in virtù della loro natura di dati particolarmente sensibili, rilevanti implicazioni per la privacy e la sicurezza dei cittadini.

> Più nello specifico esso, confermando la **liceità di strumenti di riconoscimento biometrico "non in tempo reali" previa acquisizione del consenso** informato dell'interessato, introduce un **generale divieto di utilizzo dei sistemi di identificazione o categorizzazione biometrica a distanza e "in tempo reale"** per la sorveglianza di massa in spazi pubblici, **il quale può essere arginato solo in presenza delle speciali circostanze** di cui all'art. 5, co. 2 del regolamento – tra cui figurano, la ricerca di persone scomparse, la prevenzione di reati gravi e l'identificazione di persone in situazioni di vulnerabilità – o, comunque, solo se sussistono garanzie adeguate e proporzionate per la protezione dei diritti e delle libertà individuali.

In ogni caso, in conformità a quanto disposto in materia dal GDPR, il ricorso a detti strumenti presuppone **una rigorosa valutazione da parte delle autorità competenti** le quali, al termine di una serie di test e verifiche, dovranno non solo valutare la loro accuratezza ed affidabilità, per ridurre al minimo il rischio di errori di identificazione o discriminazioni, ma anche assicurare la sicurezza dei dati biometrici così raccolti e archiviati.

Riflessioni conclusive

Allo stato, pertanto, sono evidenti le **difformità applicative verificatesi in materia di riconoscimento biometrico** non solo tra i Paesi europei ed extra-europei, ma anche all'interno dell'Unione europea stessa. Emblematico, al riguardo, è ciò che sta accadendo in Italia dove, mentre **nell'aeroporto di Linate viene ufficializzata l'introduzione dei "*FaceBoarding*"** – varchi di imbarco *self-service* che promettono di ridurre i tempi del controllo dei documenti – negli stessi giorni il Garante ha, di contro, avviato **un'istruttoria sull'eventuale introduzione di un sistema di videosorveglianza, basato sulla medesima tecnologia, all'interno della metropolitana di Roma** volto ad identificare "azioni scomposte" di soggetti già noti per aver commesso "atti non conformi".

In conclusione, l'unico dato pacifico è la proroga fino al 31.12.2025 della moratoria sull'istallazione di strumenti di sorveglianza biometrica, in luoghi pubblici o aperti al pubblico, da parte degli enti pubblici e privati il cui utilizzo, dunque, rimane al momento **esclusivo appannaggio dell'autorità giudiziaria** nell'esercizio delle proprie funzioni.

Note

[1] Working Party ex art. 29, *Opinion 4/2007 on the concept of personal data*, 20 giugno 2007, 01248/07/EN – WP 136, in particolare, si veda alla fine di pag. 8 e all'inizio di pag. 9, qui. Più di recente, B. Saetta, *Dati Biometrici*, 2 marzo 2020, disponibile a questo link.

[2] Autorità Garante della Privacy, *Verifica preliminare. Riconoscimento via webcam dei partecipanti a corsi di formazione in diretta streaming – 26 luglio 2017*, consultabile qui.

[3] Sul riconoscimento facciale, cfr. il Considerando 51 Regolamento europeo n. 2016/679, consultabile qui.

[4] Obbligo di svolgere una DPIA esteso a tutti i casi di trattamento sistematico di dati biometrici, *Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 – 11 ottobre 2018,* consultabile qui.

[5] Al riguardo, sanzione GDPR disposta dall'Autorità svedese nel 2019, consultabile qui, e i principi ribaditi a più riprese anche dall'Autorità italiana: il caso Sportitalia e il caso L'Igiene Urbana Evolution s.r.l. in materia di rilevazione presenze in ambito lavorativo (**9995680, 9995701, 9995741, 9995762, 9995785**)

[6] Agencia Española Protección Datos, *14 equívocos con relación a la identificación y autenticación biométrica*, 23.06.2020, consultabile qui.

[7] News EDPB, "*Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology*", 26.01.2021, consultabile qui.

[8] Per saperne di più, consultare questo link.