

Biometria: controllo accessi e autenticazione sicura

“ Secondo numerosi esperti, il futuro della security passa dalla biometria. E questo è tanto più vero per ciò che riguarda il controllo accessi.

Esistono numerosi sistemi di identificazione in base a caratteristiche biologiche che rendono una persona unica. **Le impronte digitali** sono il sistema forse più antico e comune. **Il riconoscimento facciale**, dell'iride o delle vene del palmo, anch'esse uniche per ogni individuo, sono invece soluzioni contactless che si sono diffuse soprattutto durante e dopo la pandemia da Covid-19. Ma esistono anche il riconoscimento della voce, dell'andatura e, tecnologia che sembra uscita pari pari da *2001 Odissea nello spazio*, delle emozioni.

AI e biometria

Proprio come nel film cult di Kubrick, che peraltro risale all'ormai remoto 1968, anche nella biometria, oggi, anno 2023, gioca un ruolo fondamentale **l'intelligenza artificiale**. Che viene utilizzata, ad esempio, per un'analisi più accurata delle impronte digitali o per **il riconoscimento facciale tridimensionale**, con algoritmi che consentono di identificare le persone anche quando subiscono cambiamenti come la chirurgia plastica o la crescita di barba e baffi. Inoltre l'intelligenza artificiale consente di ricostruire esattamente un volto anche se è parzialmente coperto da una mascherina.

Maggiore precisione

Con l'intelligenza artificiale, **l'autenticazione biometrica ha fatto un salto tecnologico notevole**. Perché gli algoritmi consentono una precisione e una reattività che superano di gran lunga le capacità umane, valutando modelli complessi in una frazione di secondo. Ciò significa un controllo degli accessi più affidabile e tempestivo per il personale addetto alla sicurezza fisica. Ad esempio, è possibile identificare piccole differenze nella struttura del viso o nelle impronte digitali in frazioni di secondo.

Per scaricare il report di Technavio



Mercato in crescita

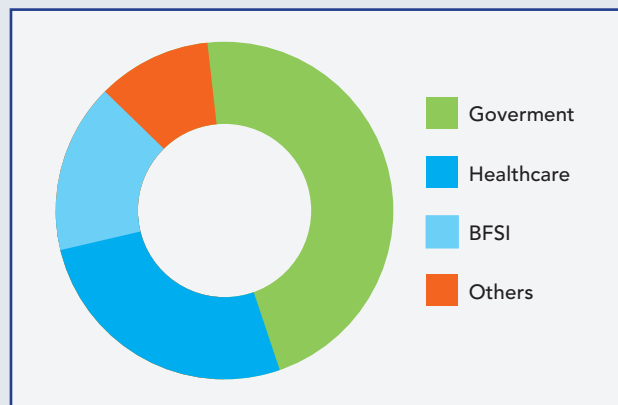
E, infatti, il mercato globale della biometria è in continua ascesa. Secondo Technavio si parla di **un CAGR di 12.85% tra il 2022 e il 2027** e si prevede che la dimensione del mercato aumenterà di 27.436,19 milioni di dollari.



Fonte: Technavio

Quali utenti?

Decisamente interessante è anche vedere la segmentazione di questo mercato per end user. Se, infatti, **Enti Pubblici detengono le fette principali della torta**, anche il settore che viene definito come BFSI (Banking, Financial Services and Insurance) e quello della Sanità ne prendono un bel pezzo. I dati parlano chiaro: c'è una crescente domanda di sicurezza e la risposta può passare proprio dalla biometria. Perché, rispetto ai metodi di identificazione e controllo tradizionali, fornisce un sistema più affidabile.



Fonte: Technavio

Killer application

Secondo gli analisti, allo stato dell'arte la cosiddetta "killer application" è proprio la tecnologia di riconoscimento facciale, che consente, tra l'altro, di identificare i criminali, di rilevare gli ingressi autorizzati e di monitorare gli spazi. E questo sia negli ambienti pubblici sia in quelli privati ma "ad alto rischio", come il settore finanziario. Inoltre, la diffusione massiccia di **smartphone che si sbloccano proprio tramite il riconoscimento facciale ha dato un notevole impulso non solo alla ricerca tecnologica, ma anche ad un'accettazione tecnologica massiva.** Recenti statistiche evidenziano che oltre l'80% degli smartphone monta una qualche forma di protezione biometrica, e che rispetto a qualche anno fa il numero di utenti che utilizzano questo sistema è aumentato del 68%. Ci siamo abituati: visto che ci facciamo riconoscere tramite il viso dal nostro telefonino, perché non accettare lo stesso sistema per entrare in un ufficio pubblico o in una banca?

Governativo

Certo, **il segmento governativo** è quello che mostra la crescita maggiore: i passaporti, le carte d'identità, i visti ormai implementano tecnologie biometriche per la verifica delle identità dei cittadini. E, nello stesso tempo, anche l'accesso agli uffici e ai "palazzi del potere" prevede da tempo la sostituzione delle vecchie tecnologie di controllo con quelle biometriche, più sicure, veloci e affidabili. E' per questo motivo che, a parere degli esperti, sarà ancora per qualche anno questo settore a guidare la crescita del mercato.

Sanità

Nel **settore sanitario**, la tecnologia biometrica viene utilizzata per vari scopi, come l'identificazione dei pazienti, il controllo degli accessi e il monitoraggio. La **sicurezza e la privacy dei dati sanitari**, per loro natura molto sensibili, è sempre stata una preoccupazione. Per impedire accessi fraudolenti, sia fisici sia informatici, a queste informazioni, si utilizzano oggi processi di autenticazione a più fattori, almeno uno dei quali è sicuramente biometrico.

Trasporti

La biometria è diventata una parte essenziale dell'autenticazione anche nel **settore trasporti**: molti terminali aeroportuali hanno adottato la tecnologia di riconoscimento facciale come un modo efficiente per verificare l'identità dei passeggeri fornendo un check-in più rapido e utilizzare le credenziali memorizzate anche per ripetere una prenotazione.

Hotel

E perfino **il controllo degli accessi in un hotel** può avvenire tramite un sistema biometrico molto semplice: un selfie, ad esempio, permette di prendere direttamente le chiavi della camera e gli algoritmi del software di identificazione sono in grado di riconoscere una foto vera da una falsa.

I componenti

Ma quali sono i componenti di un sistema biometrico? Per la parte hardware, si parte dagli **scanner**, che possono essere utilizzati per acquisire sia le impronte digitali che quelle vocali, le caratteristiche del viso o dell'iride. Poi, ci sono le **videocamere**, che acquisiscono immagini del volto, degli occhi o di altre parti per l'autenticazione, appunto, "visiva". Questi dispositivi oggi si trovano spesso negli aeroporti o nelle zone di controllo delle frontiere e l'evoluzione tecnologica li sta rendendo sempre più sicuri e affidabili.

Il software

E poi c'è tutta la parte del software, che oggi, grazie all'intelligenza artificiale, utilizza algoritmi per identificare quelle caratteristiche che rendono una persona unica, come la distanza tra occhi, naso, bocca, o, nel caso dell'iride, confronta il modello acquisito con un database di modelli già noti. Di solito, questi tipi di software sono molto utilizzati proprio nel controllo degli accessi, ma anche nella rilevazione presenze.

Cloud

Quali sono, quindi, i topics della biometria per il controllo accessi, oggi e nel prossimo futuro? Iniziamo dal **cloud**, per il riconoscimento facciale in tempo reale. Sulla "nuvola", infatti, si possono archiviare una grande quantità di dati utili, fra l'altro, anche proprio per le procedure di confronto ed è altresì possibile **il monitoraggio da remoto**, che è essenziale in un periodo post pandemia dove il lavoro ibrido è ancora presente.

Autenticazione a più fattori

Il secondo trend è rappresentato **dall'autenticazione a più fattori**, cui già abbiamo fatto cenno, che si appresta a diventare la norma. Già ampiamente usata per i dati sensibili tipo, appunto, quelli sanitari, questa tecnologia combina una tradizionale chiave di accesso, o una password, con la biometria, sia delle impronte sia facciale. Oggi, con l'aumento dei crimini informatici, si rende sempre più necessario proteggere ogni tipo di dato, non solo quelli ad alto rischio.

Contactless

Poi, abbiamo **la biometria contactless**, diventata un must dopo la pandemia: combinata con sistemi e algoritmi integrati, consente alle persone di spostarsi senza problemi e senza sacrificare la sicurezza. I più recenti sistemi biometrici, ad esempio, possono pre-autorizzare una persona a entrare in un edificio, informare le persone interessate del suo arrivo e chiamare un ascensore, il tutto senza dover toccare nulla...

Privacy compliance

E, infine, si parla sempre di più di **"biometria etica"**, perché va bene la sicurezza, ma ormai siamo tutti più attenti alla protezione dei nostri dati, e che i sistemi che ci proteggano garantiscano anche la nostra privacy.

In effetti, la conformità alle leggi associata all'evoluzione delle tecnologie biometriche rappresenta, oggi, la principale sfida per i player del settore. I dati, visto che riguardano strettamente la persona, sono infatti soggetti, in tutto il mondo, Italia compresa, **a leggi e regolamenti** come **il GDPR e le altre normative sulla privacy**. Se si sfogliano i giornali, sempre più spesso si trovano casi di aziende condannate per avere utilizzato in modo improprio i sistemi biometrici di controllo accessi. Insomma, la medaglia ha, come sempre, un dritto e un rovescio e bilanciare le diverse esigenze di privacy e di sicurezza, è cosa ben nota, non sempre è facile.

