Analytical Dossier 08/2025 ISSN 2704-6419

INTELLIGENCE ANTITERRORISMO:

Migliorare la sicurezza nazionale attraverso strategie biometriche proattive

Sara Osimani

International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)

First Edition: February 2025

Analytical Dossier 08/2025 - ISSN 2704-6419

www.vision-gt.eu
info@vision-gt.eu

Analytical Dossier 08/2025 ISSN 2704-6419

INTELLIGENCE ANTITERRORISMO:

Migliorare la sicurezza nazionale attraverso strategie biometriche proattive

Sara Osimani

Vision & Global Trends - International Institute for Global Analyse

INTELLIGENCE ANTITERRORISMO:
Migliorare la sicurezza nazionale attraverso strategie biometriche proattive

Sara Osimani

Introduzione

L'attacco terroristico perpetrato l'11 settembre sul suolo statunitense ha rappresentato un evento spartiacque nella storia globale.
Da allora, il terrorismo, in particolare di matrice jihadista, e diventato un tema centrale per la sicurezza nazionale e globale e per questo la comunità internazionale ha messo in atto nuove strategie per arginare un fenomeno che sembrava inarrestabile.
Le organizzazioni terroristiche sono percepite come una grande minaccia per l'ordine globale, anche se gli attacchi terroristici non sono tra le principali cause di morte a livello globale, questo perché il loro potere si basa proprio sul terrore.
Ciò significa che le società civili sono permeate dalla paura di un possibile attacco terroristico, in quanto in quest'ultima fase del terrorismo transnazionale gli obiettivi sono inaspettati, non specifici e soprattutto luoghi di vita comune.
Inoltre, il terrorismo jihadista è una minaccia transnazionale che attraversa i confini e implica la necessità di una cooperazione internazionale tra gli Stati e le agenzie antiterrorismo, al fine di attuare misure efficaci che possano contrastare il fenomeno e costruire una più forte percezione di sicurezza tra la popolazione.
I governi, le organizzazioni internazionali e le agenzie del settore stanno infatti mettendo in atto misure proattive che si concentrano sull'anticipazione e la prevenzione delle minacce.
Nel contesto dell'antiterrorismo, le misure proattive includono l'uso di strumenti tecnologici all'avanguardia, necessari per far fronte all'evoluzione tecnologica parallela che sta caratterizzando le organizzazioni terroristiche.
Il presente documento si concentra sull'applicazione della tecnologia biometrica come strumento di contrasto al terrorismo in diverse aree critiche e ne analizza le implicazioni e l'efficacia nella prevenzione del fenomeno.

Biometria

L'International Organization for Standardization (ISO), in quanto principale organizzazione internazionale che sviluppo standard globali anche nel campo della sicurezza informatica, definisce la biometria come "il riconoscimento automatizzato di individui basato sule loro caratteristiche biologiche e comportamentali" (National Cyber Security Centre, 2019).
L'identificazione personale è necessaria per garantire la sicurezza delle informazioni critiche in qualsiasi settore e nei governi e consiste fondamentalmente in un processo di verifica della compatibilità di un individuo con la sua identità dichiarata.
Poiché le frodi e i furti di identità rappresentano una sfida significativa per l'identificazione e, di conseguenza, minano la salvaguardia dei dati critici e riservati, un numero sempre maggiore di organizzazioni sta passando a sistemi di autenticazione automatica dell'identità (A. Jain, 2000).
I metodi di autenticazione automatica tradizionali si basavano su *token* – token fisici come documenti d'identità carte di credito o chiavi - o su processi cognitivi - basati su password o su informazioni personali, come nel caso delle domande di sicurezza (A. Jain, 2000).
Il riconoscimento automatico dei soggetti attraverso la biometria invece si basa sull'associazione delle caratteristiche distintive di una persona dati biometrici precedentemente raccolti e poi archiviati in database.

Tra le caratteristiche morfologiche personali che possono essere raccolte come dati biometrici vi sono i tratti del viso, le impronte delle dita e del palmo della mano, la retina dell'occhio e l'impronta dell'iride, il DNA, il sangue, la voce, la geometria della mano e delle dita e la firma, in quanto sono elementi unici e permanenti che caratterizzano una persona (UN, s.d.).
La fase di raccolta di questi campioni è denominata modulo di *enrollment*, durante il quale gli identificatori biometrici vengono scansionati grazie a un sensore biometrico, elaborati attraverso un software di estrazione delle caratteristiche che genera il template con cui l'individuo viene confrontato durante l'autenticazione.
I modelli risultanti vengono quindi memorizzati in un database del sistema biometrico e, durante la fase di riconoscimento, vengono confrontate con le caratteristiche biometriche degli individui in questione ed elaborati da un software *feature matcher* che stabilisce se le caratteristiche distintive corrispondono (A. Jain, 2000).

Applicazioni

Poiché la società odierna fa sempre più affidamento sui dati, sulle nuove tecnologie e sul cyberspazio, la sicurezza di questo settore è diventata fondamentale e l'analisi biometrica rappresenta un possibile strumento per migliorarla nel settore sia pubblico che privato.
L'applicazione più nota per l'autenticazione biometrica nella sicurezza dei dati è stata introdotta dalla Apple nel 2017 con il sistema Face ID (Apple, 2017).
L'allora nuovo iPhone X era stato implementato con un sistema che, basandosi sulla raccolta e sul riconoscimento delle caratteristiche biometriche del proprietario del dispositivo, consentiva l'accesso ai suoi dati.
In questo modo la multinazionale non solo garantiva una migliore funzionalità e accessibilità al dispositivo, ma anche il più alto livello di sicurezza.
Apple Face ID si basa sulla tecnologia della fotocamera TrueDepth che mappa i dettagli morfologici del volto dell'utente che vengono poi memorizzati come rappresentazione matematica che ha anche la possibilità di adattarsi ai cambiamenti dell'aspetto dell'utente (Apple, 2017).
Ciò ha segnato un'evoluzione nell'uso della biometria che iniziato ad essere utilizzata progressivamente anche in ambito di sicurezza interna.
Uno dei principali esempi e l'integrazione delle tecnologie biometriche nella governance delle frontiere, che nel contesto della sorveglianza dei confini nazionali facilita i processi di monitoraggio per le autorità.
In questo caso i dati biometrici vengono raccolti da autorità di migrazione, aziende private, organizzazioni internazionali e Stati e poi archiviati in database globali per migliorare la sicurezza dei confini e la cooperazione della comunità internazionale in materia.

Sempre nell'ambito della sicurezza nazionale, il documento si concentrerà ora sull'integrazione delle tecnologie biometriche nello sviluppo di misure proattive di lotta al terrorismo da parte della comunità internazionale.
Innanzitutto, è necessario identificare le aree critiche relative alle minacce terroristiche in cui la sorveglianza e il monitoraggio basati sulla biometria potrebbe portare a un aumento significativo della sicurezza.

Sicurezza aeroportuale

Soprattutto dopo l'attacco dell'11 settembre, gli aeroporti sono stati considerati la principale infrastruttura sensibile agli attacchi terroristici.
In particolare, le aree con accesso limitato al personale autorizzato devono essere strettamente monitorate e il processo di autenticazione basato su token lascia spazio ad accessi non autorizzati che possono essere effettuati tramite la falsificazione, il furto o l'errata collocazione dei relativi token.
In questo caso, l'implementazione di sistemi biometrici di autenticazione garantisce un maggiore livello di sicurezza di queste aree e delle informazioni e infrastrutture sensibili che contengono (Woodward, 2001).
Le stesse vulnerabilità si applicano a passaporti, carte d'imbarco e visti. La falsificazione dei documenti, il furto di identità e le frodi sono una delle principali preoccupazioni per la sicurezza aeroportuale e, in generale, nazionale.
La questione è stata affrontata con l'integrazione di controlli basati sulla biometria, principalmente il riconoscimento facciale e delle impronte digitali, che rendono più difficile superare con documenti falsi (Woodward, 2001).
La pandemia da Covid in questo campo ha segnato uno spartiacque, in quanto le restrizioni, tra cui le maschere per viaggiare e la possibilità di trasmettere o essere trasmessi dalla malattia attraverso il contatto, hanno favorito l'integrazione di sistemi biometrici di riconoscimento, come gli scanner dell'iride o delle impronte digitali, la cui efficienza non è stata influenzata dalle misure restrittive.
Questo ha portato all'innovazione dei sistemi di sicurezza negli aeroporti e alle successive evoluzioni.
Inoltre, negli ultimi anni la tecnologia biometrica p stata integrata nei passaporti stessi, creando i cosiddetti passaporti elettronici.
A livello tecnico, i passaporti elettronici sono generati incorporando nei tradizionali documenti fisici dei chip elettronici che memorizzano i dati personali e le caratteristiche delineate nella seconda pagina del passaporto.
Negli Stati Uniti, ad esempio, i chip contengono un'immagine digitale dell'individuo, la relativa impronta digitale e/o la scansione dell'iride, in modo che ogni volta che qualcuno passa attraverso i controlli di sicurezza aeroportuale l'identità venga verificata attraverso i dati biometrici (ICAO, n.d.).
Gli *ePassport* sono inoltre dotati di una firma digitale unica, specifica per ogni Paese, che fornisce un ulteriore livello di protezione dei dati in quanto la validità della firma digitale è ancorata all'autorità dello Stato o dell'Organizzazione che rilascia il passaporto elettronico, sotto la responsabilità del relativo punto di riferimento nazionale, la *Country Signing Certification Authority*.
Secondo l'Organizzazione Internazionale dell'Aviazione Civile (ICAO), sono almeno 140 gli Stati e le entità non statali che emettono passaporti elettronici e più di un miliardo quelli in circolazione (ICAO, n.d.).
Questa tecnologia rafforza la sicurezza delle frontiere e la sicurezza nazionale nel contesto delle strategie di contrasto al terrorismo.

Un'altra area critica in cui i programmi di autenticazione biometrica automatizzata potrebbero essere una risorsa preziosa, e di fatto stanno venendo progressivamente integrati, è l'identificazione di terroristi noti o sospetti attraverso i sistemi di sorveglianza.

Applicazione da parte delle Organizzazioni Internazionali

Nazioni Unite

Gli attori del settore pubblico che si sono affidati a questa tecnologia includono agenzie e organizzazioni che operano nel campo alle forze dell'ordine, della giustizia penale, della sicurezza, dell'immigrazione e dell'assistenza sociale. La diffusione della sua applicazione nel settore pubblico è iniziata formalmente dal 2016, quando il Consiglio di Sicurezza delle Nazioni Unite ha adottato la Risoluzione 2322 (UN, s.d.).

L'ONU considera gli attacchi terroristici come una delle minacce più gravi alla sicurezza nazionale e alla pace con particolare attenzione alle organizzazioni terroristiche di ISIS e Al-Qaeda, e i loro affiliati, e il fenomeno collegato dei *foreign fighters* (FTF) (S/RES/2322, 2016).

Quest'ultimo aspetto è caratteristico della cosiddetta fase di collegamento nell'evoluzione del terrorismo di matrice jihadista nei paesi occidentali, poiché dalla sua fondazione nel 2014 l'ISIS ha attirato un numero importante di persone che hanno compiuto l'*hijra*[1] verso il Califfato islamico per essere addestrate e poi sono tornate nei loro paesi d'origine per diffondere la narrativa o compiere attacchi.

La natura transnazionale di questa minaccia rende necessario sviluppare e rafforzare la cooperazione internazionale nell'applicazione di misure antiterrorismo efficaci.

La Risoluzione ha inoltre sottolineato l'importanza di integrare le nuove tecnologie nella prevenzione e nel contenimento della minaccia terroristica, spingendo gli Stati membri a condividere le informazioni rilevanti relative ai singoli terroristi e alle organizzazioni terroristiche, compresi i dati biometrici, al fine di affrontare meglio la minaccia da essi rappresentata (S/RES/2322, 2016).

L'uso dell'autenticazione biometrica è poi citato dal Consiglio di Sicurezza nelle Nazioni Unite nella Risoluzione 2396, adottata nel 2017, che invita gli Stati a implementare questa tecnologia come parte delle misure proattive per contrastare la minaccia terroristica e in particolare gli FTF (S/RES/2396, 2017).

Come già accennato, l'integrazione di tecniche di autenticazione biometrica garantisce un ulteriore livello di sicurezza nel controllo delle frontiere nazionali e contro le frodi e i furti d'identità attraverso la falsificazione di documenti d'identità.

La Risoluzione sottolinea poi la necessità di integrare i sistemi di raccolta dei dati biometrici e di condividere le informazioni necessarie nei database globali e nelle liste di sorveglianza delle persone di interesse.

Queste liste di sorveglianza e database sono abbinate ad altre tecnologie emergenti come telecamere ad alta definizione, algoritmi in grado di abbinare elementi biometrici, intelligenza artificiale e la biometria è stata persino integrata nel sistema di alcuni aerei senza pilota (UAV) nel contesto della sorveglianza delle frontiere o delle operazioni di polizia (CTED, 2021).

Ciò consente di individuare eventuali persone di interesse, sospette o conosciute, anche negli spazi pubblici.

Secondo un documento analitico della Direzione esecutiva del Comitato antiterrorismo (CTED) (CTED, 2021), si nota una tendenza positiva nell'applicazione delle tecnologie biometriche tra Stati membri, soprattutto nel contesto della cooperazione internazionale.

[1] Nel mondo islamico l'*hijra* si riferisce alla migrazione o pellegrinaggio, nel caso dell'ISIS alla migrazione verso il Califfato islamico.

Infatti, i dati biometrici raccolti dagli Stati membri dovrebbero essere condivisi con gli altri attori statali interessanti, ma la stessa importanza viene data anche alla cooperazione con INTERPOL (S/RES/2396, 2017).
In questo modo gli attori potrebbero sviluppare un sistema di controllo incrociato basato su banche dati sul terrorismo e banche dati biometriche.
Il contributo e l'utilizzo dei database biometrici di INTERPOL è estremamente importante per l'attuazione di misure di prevenzione e sorveglianza efficaci nel contesto del contrasto al terrorismo.

INTERPOL
L'INETERPOL è stata istituita nel 1923 come Commissione Internazionale di Polizia Criminale (ICPC) con l'obiettivo di prevenire e combattere il crimine attraverso una maggiore cooperazione e innovazione in materia di sicurezza.
Attualmente l'INTERPOL può contare su 196 Stati partner che collaborano principalmente attraverso lo scambio di dati di polizia per supportare le azioni di contenimento del tasso di criminalità a livello globale, l'INTERPOL può di fatti contare su 19 banche dati globali.
La raccolta dei dati e la cooperazione tra i Paesi è rafforzata dall'istituzione dei *National Central Bureaus* (NCB), che sono gli uffici locali di INTERPOL in ogni Paese membro e sono responsabili della raccolta dei dati, della distribuzione dei compiti e dei report alla sede centrale di Lione.
Il contrasto del terrorismo transnazionale è uno degli obiettivi principali dell'organizzazione e la sua struttura la rende uno degli attori globali fondamentali di questo settore.

Strategia globale antiterrorismo 2022-2025
L'implementazione di strumenti tecnologicamente innovativi è un asset fondamentale per contrastare il terrorismo, ma è anche necessario considerare che le stesse innovazioni possono essere impiegate dalle organizzazioni terroristiche, per cui essendo le minacce in continua evoluzione anche le misure di prevenzione e contrasto devono esserlo.
Per questo motivo la Direzione antiterrorismo di INTERPOL ha emanato la Strategia globale antiterrorismo 2022-2025, che ha l'obiettivo di sostenere il sistema internazionale di applicazione della legge nell'affrontare le minacce poste dai terroristi e dalle organizzazioni terroristiche.

La strategia si basa su quattro pilastri principali:
- La condivisione rafforzata dei database di polizia sulle persone di interesse nel contesto del terrorismo;
- Migliorare la consapevolezza dei Paesi membri sull'evoluzione delle minacce;
- Implementare un approccio multi-agenzia che possa fornire ai Paesi membri competenze tecniche;
- Delineare le priorità e le esigenze della comunità internazionale delle forze dell'ordine nella sua azione di contrasto al terrorismo (INTERPOL, 2021).

Questi obiettivi possono essere raggiunti attraverso l'attuazione di un approccio che la Direzione ha creato sulla base delle "3B" (INTERPOL, INTERPOL Annual Report 2023, 2023):
- Sicurezza delle frontiere (*Border security*)
- Raccolta di dati biometrici (*Biometric Data Collectio*n)
- Scambio di informazioni sul campo (*Battlefield Information Exchange*)

Ancora una volta, la biometria è considerata uno strumento prezioso per l'implementazione di misure proattive contro il terrorismo, in quanto offre la possibilità di individuare con precisione e rapidità individui sospettati o noti per essere collegati ad azioni terroristiche e di conseguenza fornire i dati necessari alle autorità competenti per monitorarli o agire.

L'aspetto più interessante della questione è che i database di INTERPOL sono disponibili a livello globale e di provenienza globale, e questo dà la possibilità di stabilire un sistema decentralizzato e focalizzato sulle regioni.
Questo modello è la miglior opzione possibile per contrastare un fenomeno transnazionale come quello del terrorismo di matrice jihadista.
Infatti, la polizia locale ha ricevuto formazione e strumentazione mobile al fine di registrare i dati biometrici delle persone condannate per reati legati al terrorismo e di caricarli nei database di INTERPOL che possono essere consultati dalle autorità di polizia di tutti i paesi partner (INTERPOL, n.d.).

Hub Biometrico
Il settore di autenticazione e identificazione biometrica interno all'INTERPOL è stato ulteriormente implementato con il lancio, nell'ottobre del 2023, del Hub Biometrico (INTERPOL, 2023).
L'Hub Biometrico è stato integrato come parte del programma decennale I-Core, che ha l'obiettivo di rafforzare le strategie internazionali e transnazionali di contrasto alle minacce alla sicurezza nazionale poste da criminalità organizzata e terrorismo, attraverso un sistema di cooperazione rafforzata che si basa sullo sfruttamento dei vantaggi offerti dall'evoluzione tecnologica (INTERPOL, 2023).
Questo progetto rappresenta una risorsa senza precedenti per il riconoscimento biometrico basato su un database internazionale che è diventato uno strumento fondamentale nell'antiterrorismo e anche nelle normali operazioni di polizia (INTERPOL, 2023) e che in una seconda fase sarà anche applicato alla governance dei confini al fine di supportare le autorità di controllo dei confini nel compito di monitoraggio delle frontiere come prima linea di protezione contro le minacce, in particolare gli FTF, e al tempo stesso una delle maggiori vulnerabilità.
Grazie a questo programma, le autorità statali hanno la possibilità di caricare scanner di impronte digitali e palmari e immagini facciali sull'Hub Biometrico dove queste vengono confrontate ai dati presenti nel database biometrico dell'INTERPOL di riconoscimento sia facciale che digitale, attraverso un software di confronto di immagini al fine di cercare possibili corrispondenze (INTERPOL, n.d.).
Il software alla base del funzionamento di questo sistema è stato progettato da IDEMIA, un'azienda francese che ha fornito tecnologia all'avanguardia all'INTERPOL per più di vent'anni.
IDEMIA Multibiometric Identification System (MBIS) 5 è un software che vanta un algoritmo di ultima generazione che garantisce una performance migliorata e un'interfaccia più user-friendly (IDEMIA, 2023).
Il fatto che i dati caricati siano confrontati con i due database allo stesso tempo attraverso una singola interfaccia garantisce una risposta immediata e precisa e di conseguenza permette un'azione pronta ed efficace in caso di corrispondenza.
Inoltre, il processo è quasi completamente automatizzato con l'intervento di operatori che si rende necessario solo nel caso in cui i dati biometrici caricati non rispettino il livello minimo di qualità di immagine del programma.

Un primo successo dato dall'implementazione dell'Hub Biometrico è stato raggiunto nel 2023 nel contesto dell'Operazione HOTSPOT.
HOTSPOT consiste in un'iniziativa lanciata dall'INTERPOL che si basa sull'analisi di dati biometrici raccolti dalle autorità che monitorano i flussi che attraversano i confini di Iraq, Moldavia, Repubblica Ceca, Ungheria, Slovenia, Serbia, Montenegro, Macedonia del Nord, Bosnia-Erzegovina e Albania (INTERPOL, 2023).

Inizialmente i dati raccolti vengono caricati in database separati per la corrispondenza delle impronte digitali e delle immagini facciali, implicando un processo più complicato e lento, mentre con l'introduzione dell'Hub Biometrico la possibilità di poter contare su un database comprensivo fornisce una risposta più immediata e accurata (INTERPOL, Biometric Hub, n.d.).
Questo è stato evidente subito dopo l'integrazione del nuovo strumento, quando durante un controllo di polizia a Sarajevo, in Serbia, i dettagli biometrici di un contrabbandiere di migranti sono stati caricati nell'Hub Biometrico e risultati in una corrispondenza con una persona di interesse ricercata in un altro paese europeo per crimine organizzato e traffico di esseri umani dal 2021.
Il contrabbandiere ha fornito alla polizia un passaporto fraudolento e un nome falso, mah grazie all'analisi dei dati biometrici la sua identità è stata verificata e le autorità hanno potuto agire di conseguenza (Zulhusni, 2023).
L'evoluzione del programma lo porrebbe come uno strumento rivoluzionario nel contesto del contrasto al terrorismo in quanto permette di controllare immediatamente se una persona potrebbe essere una minaccia alla sicurezza nazionale sulla base di informazioni raccolte nei 196 paesi partner, quindi con una proiezione globale.
In particolare, nel contesto degli FTF, ma in generale con individui collegati a organizzazioni o attività terroristiche, l'Hub Biometrico e le tecnologie biometriche in generale aggiungono concretamente uno strato di sicurezza che potrebbe effettivamente ridurre al minimo le minacce risultanti dalla produzione e utilizzo di documenti falsi e dal contrabbando di migranti.

È necessario menzionare che una delle *notice* che l'INTERPOL può emettere, e che avvisa le autorità in caso di corrispondenza dei dati biometrici, è *la Special INTERPOL-UN Security Council Special Notice* che viene emessa per individui ed entità che sono target di sanzioni del Consiglio di Sicurezza delle Nazioni Unite, tra cui chiunque sia collegato ad Al-Qaeda e all'ISIS, e delinea le sanzioni relative che devono essere applicate a questi specifici individui o entità (INTERPOL-United Nations Security Council Special Notices, n.d.).
A partire dal 2017 l'INTERPOL e le Nazioni Unite hanno promosso il caricamento di dati biometrici per supportare l'emissione di Special Notices (INTERPOL-United Nations Security Council Special Notices, n.d.).

Questo è un chiaro esempio mi come la biometria si è riconosciuta internazionalmente come uno strumento essenziale per l'implementazione di strategie di controterrorismo nello spazio pubblico e permette, non solo di contrastare, ma anche di prevenire l'ingresso di possibili minacce nel territorio nazionale.

Sfide
Come ogni tecnologia la biometria pone anche delle sfide, oltre a dei vantaggi.
Dal punto di vista etico, i sistemi biometrici sono basati sulla raccolta di caratteristiche fisiche di individui e di conseguenza una delle principali problematiche riguardante questo settore sono le questioni etiche che solleva in quanto rischia di violare il diritto fondamentale alla privacy.
Per esempio, l'Hub Biometrico dell'INTERPOL ha sviluppato un sistema per cui i dati raccolti sul campo non sono immagazzinati nel database criminale, né accessibili da altri attori, e se non risultano in una corrispondenza vengono immediatamente cancellati.
Questo può essere un metodo efficace per rispettare le politiche di privacy dei dati, ma comunque la progressiva integrazione di questa tecnologia restringe il campo della privacy della popolazione civile e le autorità competenti devono continuare a sviluppare regolamenti e linee guida al fine di proteggere il diritto della privacy, specialmente durante il mantenimento dei dati dopo la raccolta.

Le autorità che hanno integrato tecnologie biometriche nelle loro strategie devono tenere in considerazione che la tecnologia può essere, e probabilmente è già stata, utilizzata dal crimine organizzato o da organizzazioni terroristiche, specialmente attraverso attacchi cyber, che possono utilizzare i dati biometrici con intenzioni illegittime.
Questo è anche dato dal fatto che le organizzazioni e i soggetti criminali, al contrario degli Stati o delle agenzie internazionali, non devono rispettare la legge e i diritti umani e di conseguenza possono utilizzare le innovazioni tecnologiche nel modo peggiore ma anche più efficace.
Questo può essere affrontato solamente con una collaborazione e cooperazione trasparente e solida tra gli Stati e le agenzie, che si deve basare sulla condivisione di dati e informazioni.

Nonostante gli incredibili ed esponenziali progressi nella tecnologia alla base dei sistemi biometrici e dei relativi programmi, la variazione di elementi ambientali durante la raccolta dei dati potrebbe portare a un risultato poco affidabile.
Le due macrocategorie di errori in questo campo sono le false corrispondenze - nel caso in cui il sistema mostri una falsa corrispondenza tra i dati raccolti e i dati immagazzinati nel database biometrico - o le false non corrispondenze - nel caso in cui il processo risulti in una mancata corrispondenza nonostante l'individuo effettivamente corrisponde ai dati biometrici che sono immagazzinati nel database (National Cyber Security Centre, 2019).
Questo potrebbe portare a conseguenze estremamente serie dato che le autorità si stanno progressivamente affidando ai risultati dati dai sistemi biometrici.

Conclusioni

Per concludere è possibile affermare che mentre le minacce poste dalle organizzazioni terroristiche transnazionali e dagli FTF evolvono continuamente e non esiste uno strumento di contrasto e prevenzione efficace al cento per cento, la tecnologia biometrica è l'ultima è più efficiente misura proattiva che potrebbe effettivamente portare a una diminuzione del fenomeno.
Il fatto di poter contare su corrispondenze biometriche, invece di doversi affidare solamente ah token fisici per l'autenticazione dell'identità sulle frontiere o sul territorio nazionale e rivoluzionario nel contesto dell'utilizzo e produzione di documenti falsi, che comunque rappresenta una minaccia significativa per la sicurezza nazionale.
Cyril Gout, direttore esecutivo ad interim dei servizi di polizia dell'INTERPOL, ha dichiarato che se anche gli individui con intenti criminali solitamente hanno le capacità e possibilità tecniche di cambiare il loro nome, contraffare i documenti e addirittura alcuni aspetti fisici al fine di portare a compimento il loro piano senza essere scoperti dalle autorità, ma è quasi impossibile modificare i dati biometrici che caratterizzano universalmente ognuno di noi.
Questo, anche con tutte le necessarie precauzioni e vulnerabilità che devono essere affrontate, pone la tecnologia biometrica come lo strumento più affidabile ed efficace da impiegare nelle strategie di controterrorismo e, in generale, nella prevenzione del crimine.

Bibliografia

A. Jain, L. H. (2000). Biometric Identification. *Communications of the ACM, 43*(2).

Adkins, L. D. (2007). Biometrics: Weighing Convenience and National Security against Your Privacy. *Michigan Telecommunications and Tecnology Law Review, 13*(2).

Apple. (2017). *Support Apple*. Tratto da Apple: https://support.apple.com/it-it/102381

Brut, C. (2023). *Interpol's New Multi-biometric System from IDEMIA Goes Live*. Retrieved from BiometricUpdate.com: https://www.biometricupdate.com/202311/interpols-new-multi-biometric-system-from-idemia-goes-live

CTED. (2021). *CTED Analytical Brief: Biometrics and Counter-Terrorism.* Retrieved from United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED): https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf

ICAO. (n.d.). *Security and Facilitation, ePassport Basics*. Retrieved from ICAO: https://www.icao.int/Security/FAL/PKD/Pages/ePassport-Basics.aspx

IDEMIA. (2023). *IDEMIA provides INTERPOL with an enhanced Multibiometric Identification System to support its 196 member countries*. Retrieved from IDEMIA Group: https://www.idemia.com/press-release/idemia-provides-interpol-enhanced-multibiometric-identification-system-support-its-196-member-countries-2023-11-29

INTERPOL. (2021). *Counter-Terrorism Global Strategy 2022-2025.* Tratto da INTERPOL.

INTERPOL. (2023). *INTERPOL Annual Report 2023.* INTERPOL.

INTERPOL. (2023). *INTERPOL unveils new biometric screening tool*. Retrieved from INTERPOL News: https://www.interpol.int/News-and-Events/News/2023/INTERPOL-unveils-new-biometric-screening-tool

INTERPOL. (n.d.). *Biometrics for Frontline Policing*. Retrieved from INTERPOL: https://www.interpol.int/How-we-work/I-CORE-our-vision-for-change/Biometrics-for-Frontline-Policing

INTERPOL. (s.d.). *Counter-Terrorism, Future Oriented Policing Projects.*

INTERPOL. (n.d.). *INTERPOL-United Nations Security Council Special Notices*. Retrieved from INTERPOL: https://www.interpol.int/How-we-work/Notices/INTERPOL-United-Nations-Security-Council-Special-Notices

INTERPOL. (n.d.). *Biometric Hub*. Tratto da INTERPOL: https://www.interpol.int/How-we-work/Forensics/Biometric-Hub

INTERPOL. (n.d.). *Identifying terrorist suspects.* Retrieved from INTERPOL: https://www.interpol.int/Crimes/Terrorism/Identifying-terrorist-suspects

National Cyber Security Centre. (2019). *Biometric Recognition and Authentication Systems*. Retrieved from National Cyber Security Centre: https://www.ncsc.gov.uk/collection/biometrics/understanding-biometrics

S/RES/2322. (2016). *Resolution 2322.* Tratto da United Nations Security Council: https://documents.un.org/doc/undoc/gen/n16/433/54/pdf/n1643354.pdf

S/RES/2396. (2017). *Resolution 2396.* Retrieved from Security Council of the United Nations: https://documents.un.org/doc/undoc/gen/n17/460/25/pdf/n1746025.pdf

UN. (s.d.).

Woodward, J. D. (2001). Biometrics: Facing Up to Terrorism. *RAND Issue Paper IP-218*.

Zulhusni, M. (2023). *Biometric tool from INTERPOL is a game changer in capturing most wanted criminals*. Retrieved from Techwire Asia: https://techwireasia.com/2023/12/how-does-the-interpol-biometric-tool-capture-the-most-wanted/

Sara Osimani – *Dottoressa in Scienze della Mediazione Linguistica presso la Scuola Superiore per Mediatori Linguistici di Pisa, Master in Relazione Internazionale e Protezione Internazionale dei Diritti Umani presso SIOI (Società Italiana per l'Organizzazione Internazionale),* attualmente *studente magistrale in Investigazione, Criminalità e Sicurezza Internazionale, presso l'Università degli Studi Internazionali di Roma. Stagista presso Vision & Global Trends International Institute for Global Analyses, nell'ambito del progetto Società Italiana di Geopolitica*.

Vision & Global Trends - International Institute for Global Analyses

www.vision-gt.eu info@vision-gt.eu