# Il Riconoscimento Biometrico, uno strumento per l'identificazione della clientela delle Banche e degli Intermediari Finanziari.

**di Massimo Masini**

*Laureato in Giurisprudenza presso La Sapienza di Roma, proviene dal sistema bancario ove ha acquisito significative esperienze nell'ambito della Direzione Generale con particolari mansioni legate allo studio e analisi delle normative di vigilanza bancaria, valutarie e fiscali internazionali; successivamente ha intrapreso il percorso professionale che, come esperto di normative di vigilanza bancaria, nella fase di realizzazione del nuovo quadro di riferimento normativo iniziato con la deregolamentazione valutaria del 1990, ha partecipato come esperto esterno a numerosi gruppi di lavoro istituzionali presso l'allora Ufficio Italiano dei Cambi per la predisposizione delle relative normative di attuazione attinenti la liberalizzazione del movimento di capitali e quelle riferite alla nascente disciplina "antiriciclaggio"; autore di numerose dispense sui temi indicati, è stato relatore in numerosi convegni destinati al settore bancario e degli Intermediari finanziari, attualmente riveste la carica di Amministratore della* ***GPM & SAIP GROUP srl*** *società attiva nell'ambito della consulenza e*

*della formazione alle Banche nell'ambito delle tematiche legate alla normativa antiriciclaggio.*

_____

Il Riconoscimento Biometrico, uno strumento per l'identificazione della clientela delle Banche e degli Intermediari Finanziari.
La repentina avanzata del FinTech costringe gli operatori del settore finanziario, in gran parte ancora legati ai sistemi tradizionali, ad introdurre nei loro processi interni, sempre in linea con le normative primarie e i regolamenti delle Autorità di Vigilanza, quegli obiettivi di innovazione tecnologica in grado di consentire un marcato progresso nelle fasi gestionali operative dei sistemi di pagamento direttamente "interfacciati" con la corretta e istantanea identificazione della clientela.

Uno degli aspetti indispensabili per lo sviluppo di una piattaforma FinTech dedicata alle banche e agli intermediari, è indubbiamente rappresentata dalla necessità di disporre di una tecnologia che sia in grado di identificare il cliente, senza margine di errore, all'atto dell'apertura del rapporto e, successivamente, nel momento in cui, a valere sul rapporto stesso, viene richiesta l'esecuzione di una transazione in modalità remota.

Tenuto conto che nel corso del 2017 sono stati stimati, a livello mondiale, circa 500 milioni di furti di credenziali informatiche e 18 milioni di violazioni di domini, risulta evidente che le Username, gli ID, le Password, i Token, i PIN, normalmente utilizzati nelle comuni piattaforme di home-banking, non sono più sufficienti a garantire l'inviolabilità, e quindi la sicurezza, dei dati identificativi della clientela.

L’era FinTech, che prepotentemente sta entrando nell’uso quotidiano, ha il merito di favorire l’ingresso sul mercato di numerose start-up che promuovono prodotti con tecnologie digitali funzionali al settore finanziario; tra queste, numerose sono quelle che approfondiscono ed elaborano sistemi orientati a tutelare i fruitori dei servizi bancari e di pagamento in genere, adottando procedure di immediata identificazione della clientela che garantiscano la certezza e l’inviolabilità dei dati personali.

In base agli studi sulla sicurezza informatica effettuati a livello internazionale, con i contributi dei servizi antifrode al servizio di banche e finanziarie, il presidio che appare più sicuro e che fornisce adeguate garanzie di inviolabilità, è il riconoscimento che viene fornito dal riscontro *“biometrico”*.

Il ***Sistema di riconoscimento biometrico*** ha origini in Francia sin dal ‘900 come sistema strumentale alla “antropologia giudiziaria” (misurazione delle caratteristiche fisio-somatiche dei detenuti da conservare in un archivio storico per le successive identificazioni) e, quindi, sembra curioso che, a distanza di oltre un secolo, l’applicazione di tale tecnica nel settore finanziario possa essere considerata innovativa; quindi, cercheremo ora di comprendere in che modo le banche e gli altri intermediari finanziari desiderano utilizzare questo strumento come presidio alle attività fraudolente.

Tale sistema, nell’ultimo decennio, è stato utilizzato in settori diversi da quello finanziario, basti pensare ai sistemi antifurto con rilevazione delle impronte o della voce, ai sistemi di accesso aziendale, ai sistemi di accesso nell’hardware e nel settore pubblico è stata introdotta, di recente, la carta d’identità elettronica (CIE) munita di elementi per l’identificazione fisica, attraverso i dati biometrici.

Per ***riconoscimento biometrico*** si intende il riconoscimento automatico di individui basato su loro caratteristiche biologiche o comportamentali, includendo in tale accezione le nozioni di *verifica biometrica* e di *identificazione biometrica*.

Nel momento in cui il soggetto instaura un rapporto o si iscrive in un sistema che prevede il riconoscimento dell'utente attraverso il riconoscimento biometrico viene attivata la fase di *enrolment* cioè il processo attraverso il quale avviene l'acquisizione del campione biometrico con la sua memorizzazione nel sistema e con l'estrazione dei tratti (*biometric feature*) necessari per la generazione del riferimento biometrico da trattenere come campione per i confronti successivi; il campione (*biometric sample*) è la rappresentazione analogica o digitale di una caratteristica biometrica ottenuta al termine del processo di acquisizione (*biometric capture* e *biometric acquisition*) costituita, per esempio, dalla riproduzione dell'immagine di una impronta.

La *verifica biometrica* non è altro che un confronto immediato, in forma automatica, tra un modello biometrico acquisito nel momento in cui l'interessato interagisce con il sistema biometrico e un modello biometrico previamente memorizzato nel sistema e a lui riferibile (*one-to-one comparison*). Il modello (*biometric template*) è l'insieme di tratti biometrici memorizzati informaticamente nella fase della acquisizione e direttamente confrontabile con altri modelli biometrici.

Nel momento in cui l'utente accede al sistema attraverso il proprio tratto biometrico, viene attivata la fase della identificazione, attraverso l' istanza biometrica (*biometric probe*), la quale consiste nella ricerca in un archivio, per l'esecuzione del confronto biometrico automatizzato, di uno o

più dati biometrici corrispondenti al dato acquisito (*one-to-many comparison*); tale confronto (biometric comparison viene normalmente basato su metodi statistici e metriche tipiche del sistema biometrico prescelto.

Analizzate quelle che sono le principali fasi del sistema, il processo innovativo, cui la Banche e gli Intermediari finanziari sono orientate a sviluppare e/o a perfezionare , si riferisce alle procedure informatiche appositamente finalizzate alla rilevazione istantanea delle caratteristiche biologiche e/o comportamentali, interfacciandole con l'anagrafica aziendale opportunamente implementata con l'archivio degli elementi biometrici di verifica acquisiti nel corso della fase di *enrolment* .

Nel corso degli anni, con la crescente evoluzione delle normative emanate dalle Autorità internazionali e nazionali riguardanti il contrasto del riciclaggio e del finanziamento del terrorismo, l'identificazione della clientela e/o degli esecutori, nonché la tracciabilità dei dati ad essi riferiti, è stata posta in primo piano per evitare che i canali finanziari possano essere utilizzati per trasferimenti finalizzati alla esecuzione di operazioni illecite connesse a tali reati.

A tale proposito l'Unione Europea con l'emanazione della IV Direttiva contro il riciclaggio e il finanziamento al terrorismo (849/2015), recepita in Italia con il Dlgs 90/2017, e attraverso le modifiche apportate al Dlgs 231/07, ha introdotto la possibilità di effettuare il processo di identificazione della clientela con l' "*utilizzo di altri meccanismi di riscontro basati su affidabili soluzioni tecnologiche innovative (quali, ad esempio, quelle che prevedono forme di riconoscimento biometrico), purché assistite da robusti presidi di sicurezza*".

Tali disposizioni, rispetto a quanto avveniva in un recente passato, introducono novità di portata innovativa consentendo

alle Banche, quindi, anche in assenza della presenza fisica del cliente, di poter effettuare un riscontro sulla identità del cliente attraverso le metodologie informatiche riconosciute dal Regolamento UE 910/2014.

Anche il Garante per la Protezione della Privacy, già nel 2014, in occasione delle predisposizione delle Linee Guida in materia di riconoscimento biometrico e firma grafometrica, affermava che: "*L'utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici sta andando incontro a crescente diffusione, in particolare per l'accertamento dell'identità personale …….*"; questo progresso "normativo " su vasta scala , pertanto, consente alle applicazioni biometriche di essere utilizzate autonomamente o anche integrate, a supporto, con altre tecnologie come ad esempio: smart-card, chiavi crittografiche, RFID e firma digitale; quindi, la *tecnologia biometrica*, basata sulla fisionomia del soggetto, viene considerato un sistema efficace, rapido e sicuro.

L'identificazione biometrica, certamente, rappresenta una delle tematiche di eccellenza del FinTech in quanto con l'applicazione della Psd2, la diffusione dei pagamenti digitali attraverso gli smartphone o tablet, richiede presidi di sicurezza adeguati che possano rendere vani possibili frodi generate da furti di identità.

Il procedimento di acquisizione (*enrolment*) della caratteristica biometrica (*Reference template*), viene effettuato attraverso: laser, scanner, telecamere, microfoni, ecc..; esso prevede la registrazione dell'utente con la creazione di un template (*biometric sample*) che consiste, come sopra specificato, nell'acquisizione di una o più immagini o suoni relative all'individuo elaborate grazie ad un algoritmo che varia da sistema a sistema.

Le caratteristiche biometriche hanno carattere di universalità per tutti gli individui e, nello stesso tempo, ciascuna

caratteristica è univoca per ciascun individuo, esse hanno una durata temporale lunga salvo alterazioni fisiche e/o comportamentali dovute ad eventi accidentali. Esempio: *tutti hanno le dita (universalità) ma le dita di ciascuno di noi possiedono delle impronte personali (univocità) e le dita, salvo alterazioni fisiche, hanno una durata pari alla vita dell'individuo*.

Il Garante della Privacy, pur riconoscendo la liceità della raccolta dei dati biometrici, attraverso le richiamate Linee Guida del 21/5/2014, fornisce una serie di prescrizioni finalizzate all'utilizzo strettamente necessario per l'attività istituzionale fermo restando l'informativa alla clientela circa le modalità di acquisizione del dato biometrico e il suo successivo utilizzo.

In conclusione, si riporta qui di seguito le categorie e i modelli biometrici ad oggi utilizzati, fatto salvo l'esame del DNA non rilevante nel presente contesto riferito alle attività finanziarie:

**Sistemi biometrici interattivi e sistemi biometrici passivi**
La consapevolezza dell'interessato circa l'utilizzo del dato acquisito come, ad esempio, l'acquisizione della firma o la scansione della retina determinano una cooperazione del soggetto consentendo una acquisizione partecipativa; in assenza della consapevolezza da parte dell'interessato, ad esempio la registrazione della voce o la fotografia del volto a sua insaputa determinano, invece, una acquisizione passiva non consentita dalle disposizioni.

**Caratteristiche biometriche biologiche e comportamentali**
Le caratteristiche fisio-somatiche sono quelle "biologiche"; quelle di comportamento sono la firma, la voce, l'andatura.

**Caratteristiche biometriche traccianti e non traccianti**
Una caratteristica biometrica che lascia tracce sugli oggetti è l'impronta digitale e, quindi, potrebbe essere rilevata,

anche, ad insaputa del soggetto. Caratteristiche biometriche traceless sono, ad esempio, la topografia della mano, la struttura venosa del dito, la firma.

In dettaglio, ***le tecnologie biometriche fisiologiche*** attualmente sviluppate e utilizzabili all'istante come credenziali di accesso per gli account propri del settore bancario e finanziario, con esclusione del lungo e complesso esame del DNA, sono:

- ***il riconoscimento facciale*** consente di identificare le persone sulla base dell'analisi di caratteristiche specifiche del volto che non possono essere facilmente alterate; in particolare, vengono presi in considerazione macro-elementi (bocca, naso, occhi, orecchie, fronte, mento, struttura ossea) e micro-elementi (distanza tra macro-elementi o tra macroelementi e punti di riferimento, e dimensione dei macro-elementi). Durante la rilevazione dei dati, un sensore cattura un certo numero di immagini in 2D o in 3D del volto di un individuo, che vengono poi conservate in formato digitale e, mediante un algoritmo che ne registra le caratteristiche rilevanti, possono essere memorizzate e utilizzate per eventuali processi di verifica dell'identità.
- ***l'impronta digitale*** è probabilmente la più utilizzata e accettata forma di riconoscimento biometrico, ed è stata utilizzata sin dai primi decenni del Novecento in ambito della criminologia. L'ampio utilizzo dell'impronta digitale quale tecnologia di riconoscimento biometrico che riproduca la disposizione delle creste di Galton e delle valli cutanee presenti sui polpastrelli delle dita fin dalla fase prenatale, si basa su due principi basilari: l'immutabilità e l'individualità. Si tratta di un sistema considerato affidabile in grado di consentire ricerche indicizzate attraverso i più moderni sistemi di ricerca come l'*Automatic Fingerprint Identificatisi on*

*Systems – AFIS*.

- l***a geometria della mano*** rappresenta la tecnologia di riconoscimento biometrico basata sull'impronta del palmo della mano; è molto simile a quella basata sul rilevamento dell'impronta digitale. I parametri utilizzati per il rilevamento sono fattezze maggiori (quali la lunghezza e la struttura delle dita o la misura del palmo) e fattezze minori (linee, rientranze, venature, rughe e schema creste-valli), che vengono rilevate da sensori che possono essere a ultrasuono, termici o ottici. I dispositivi più utilizzati sono quelli ottici, che acquisiscono mediante una fotocamera un'immagine in 3D, che viene poi confrontata con le immagini presenti nel database.
- ***la struttura venosa della mano e delle dita*** si sviluppa generalmente nella fase pre-natale; l'acquisizione avviene tramite sensori che rilevano la forma e la disposizione delle vene delle dita, del dorso o del palmo della mano utilizzando una sorgente luminosa a lunghezza d'onda prossima all'infrarosso.
- ***la struttura vascolare della retina*** è una membrana che forma il rivestimento interno del bulbo oculare; sulla retina di ciascun individuo vi sono caratteristici pattern formati dai vasi sanguigni sul sottile nervo posizionato sul retro del bulbo oculare che processa la luce che filtra attraverso la pupilla. I sistemi di riconoscimento biometrico basati sulle caratteristiche della retina confrontano appunto il sistema dei vasi sanguigni, il cui pattern è unico.
- ***la forma dell'iride:*** i sistemi biometrici basati sulla misurazione matematica dell'iride sono costituiti da un sensore che, appositamente posizionato, illumina l'iride del soggetto sottoposto allo scan con un laser a bassa intensità; una luce infrarossa effettua la scansione dell'occhio e rileva peculiarità della struttura dell'iride, che vengono successivamente rappresentate matematicamente da un algoritmo. L'iride è costituita da

un tessuto connettivo elastico e, avendo approssimativamente 266 caratteristiche distintive, è una preziosa fonte di dati biometrici. Nella tecnologica di riconoscimento irideo, vengono utilizzate circa 173 di queste caratteristiche distintive. Infine, per effettuare il riconoscimento le caratteristiche rilevate vengono paragonate alle immagini di iridi conservate in un template.

Inoltre vi sono le ***tecnologie biometriche comportamentali***:

- ***il riconoscimento vocale*** è considerato un sistema di riconoscimento biometrico al tempo stesso fisiologico e comportamentale. Le caratteristiche vocali che vengono registrate dal sistema includono principalmente il tono, la frequenza, l'intensità e l'articolazione nasale, e vengono inoltre presi in considerazione specifici coefficienti e spettri. L'acquisizione del dato può avvenire telefonicamente o in via informatica per consentire lo "speaker recognition" da utilizzare successivamente per l'elaborazione e l'analisi "signal processing". Normalmente la verifica vocale è confortata da altro dato complementare come una PW o altro identificativo.
- ***la firma***, la cui acquisizione avviene normalmente trae l'analisi del segnale tramite i tablet grafometrici, è la tecnologia biometrica basata sul riconoscimento della firma autografa che consente di autenticare l'identità di un individuo mediante la misurazione di specifici parametri, fra i quali la calligrafia, la velocità di firma, il ritmo, l'accelerazione e la pressione.

**spunti tratti da:**

- ***Identità, identificazione e riconoscimento – Nicola Corvino – 1 giugno 2012***
- ***Viaggio nelle tecnologie che stanno per cambiare la nostra vita – Sole 24 Ore – 2015***
- ***Cyber Warfare: Verso Un Nuovo Paradigma Strategico – Stefano Ricci – 11 settembre 2017***
- ***Linee Guida del Garante della Privacy – 21 Maggio 2014***

7 gennaio 2019