LUISS

Dipartimento
di Scienze Politiche

Cattedra di Diritto dell'Informazione e della Comunicazione

I sistemi di riconoscimento biometrico: natura, trattamento e disciplina nell'ordinamento europeo e in quello statunitense

Prof. Pietro Falletta
RELATORE

Prof. Raffaele Bifulco
CORRELATORE

Diana Avendaño Grassini
CANDIDATO

Anno Accademico 2020/2021

Indice

Introduzione……..p. 5

CAPITOLO 1: I DATI BIOMETRICI NELL'ORDINAMENTO EUROPEO……...p. 10

1. L'evoluzione del dibattito europeo sui dati biometrici……..p. 10

   1.1 Le tappe definitorie del concetto di dato biometrico……p. 16

2. I dati biometrici nella prospettiva del GDPR…….p. 18

   2.1 La disciplina del trattamento……...p. 23

   2.2 Criticità e problemi: le categorie di dato biometrico……....p. 28

3. I diritti fondamentali minacciati dall'impiego dei dati biometrici…….p. 31

4. Il trattamento di dati biometrici…….p. 36

   4.1 Il trattamento di dati biometrici in ambito commerciale……..p. 38

   4.2 I sistemi di autenticazione basati sul riconoscimento biometrico in ambito lavorativo…...p. 40

   4.3 Il trattamento di dati biometrici da parte di Autorità di pubblica sicurezza……...p.41

   4.4 Il trattamento di dati biometrici da parte di istituzioni, organi, uffici e agenzie europee…p. 44

5. Ulteriori sviluppi nel diritto europeo in materia……p. 45

   5.1 Intelligenza artificiale e riconoscimento biometrico……p. 45

   5.2 Identità digitale e riconoscimento biometrico……..p. 48

CAPITOLO 2: I DATI BIOMETRICI NELL'ORDINAMENTO ITALIANO……..p. 51

1. L'evoluzione del dibattito italiano sui dati biometrici……...p. 51

2. L'adeguamento interno alla normativa europea in Italia dall'adozione del d.lgs. n. 101/2018 al "d.l. Capienze"…….p. 56

3. Gli interventi del Garante per la protezione dei dati personali in materia di biometria, dopo l'adozione del GDPR……p. 63

   3.1 Intervista al Garante per la protezione dei dati personali…….p. 69

4. Il trattamento di dati biometrici nell'ordinamento italiano……....p. 74

   4.1 Firma grafometrica……..p. 75

   4.2 Il trattamento di dati biometrici nei rapporti di lavoro…….p. 77

      4.2.1 L'uso delle impronte digitali del lavoratore per accedere ad aree protette……..p. 78

      4.2.2 Controllo di accesso fisico ad aree sensibili e macchinari pericolosi……..p. 78

      4.2.3 Autenticazione informatica ai fini del controllo di accesso o di identificazione degli utenti……...p. 79

   4.3 Il trattamento di dati biometrici da parte di Autorità di pubblica sicurezza……..…p. 80

   4.4 Applicazioni della Data protection impact assesment (DPIA)……....p. 82

   4.5 Il trattamento illecito di dati biometrici……...p. 82

CAPITOLO 3: I DATI BIOMETRICI NELL'ORDINAMENTO STATUNITENSE……....p. 85

1. La disciplina biometrica nell'era del "*Capitalismo della sorveglianza*"……...p. 85

2. L'intervento del legislatore in materia di biometria……...p. 89

2.1 La legislazione statale sui dati biometrici……p. 91

2.1.1 Il *Biometrics Information Privacy Act* in Illinois……p. 92

2.1.2 Il *Legislative House Bill 1493* di Washington……p. 94

2.1.3 Il *Capture or Use of Biometric Identifier Act* in Texas……...p. 96

2.1.4 La legislazione in materia di privacy biometrica in California e Arkansas……p. 97

2.1.5. Proposte di legge in materia di privacy biometrica a New York e nel Maryland…..p. 99

2.2 Il *Commercial Facial Privacy Act* del 2019……...p. 100

3. Il contributo della giurisprudenza dello stato dell'Illinois……...p. 101

3.1 Il caso *Rosenbach v. Six Flags Corporation*……..p. 102

3.2 Il caso *Rivera v. Google Inc*……...p. 103

3.3 Il caso *In re Facebook*……....p. 106

3.4 Il caso *Monroy v. Shutterfly Inc*……..p. 107

4. La necessità di incrementare lo standard statunitense per la protezione dei dati biometrici…p. 108

4.1 Le asimmetrie nelle leggi statali statunitensi in materia di biometria……....p. 109

4.2 L'adozione di uno standard federale per la protezione dei dati biometrici…….....p. 112

4.3 I principi del GDPR applicati alla protezione dei dati biometrici negli Stati Uniti……....p. 116

5. Il trattamento di dati biometrici da parte di autorità pubbliche nell'ordinamento statunitense…….p. 119

Conclusioni……...p. 125

Riassunto……...p. 132

Bibliografia……...p. 143

Introduzione

Nel lungo dibattito che da tempo anima la riflessione giuridica in materia di protezione dei dati personali, in genere si muove dall'assunto di fondo che i nostri dati non siano in grado di rispecchiare interamente la nostra identità. Infatti, la persona fisica non può essere semplicemente ricondotta alle sue abitudini di acquisto online, ai suoi post sui social network, a cosa guarda su Netflix e via dicendo. Vi è però un settore particolare in cui la sineddoche fra dato e persona tende a realizzarsi, quando la disciplina sulla tutela dei dati personali incrocia la materia dei dati biometrici. Se configuriamo l'identità di un individuo in senso oggettivo, come l'insieme degli elementi "misurabili" riferibili al suo corpo, la rilevazione dei suoi caratteri biometrici di fatto tenderà a coincidere con esso.

L'utilizzo del proprio corpo come strumento di riconoscimento non costituisce qualcosa di nuovo, ma è una pratica da tempo presente in ambito investigativo e giudiziario, dove i primi sistemi di rilevazione biometrica hanno trovato la loro applicazione. Negli ultimi decenni, però, il settore delle tecnologie biometriche ha subito forti innovazioni, che ne hanno determinato una loro progressiva diffusione in numerosi ambiti pubblici e privati. Attualmente, i dati biometrici sono sempre maggiormente impiegati nella vita di tutti giorni per effettuare l'accesso a determinati luoghi o servizi e consentire l'utilizzo di alcuni dispositivi elettronici negli ambiti bancari, sanitari, del commercio, dell'istruzione e delle telecomunicazioni. Queste tecnologie biometriche detengono numerosi vantaggi per l'elevata usabilità dei loro sistemi e la precisione nei processi d'identificazione automatizzati degli individui. I caratteri biometrici risultano, infatti, tendenzialmente unici e pertanto facili da utilizzare e difficili da contraffare. Questi dati che ridisegnano in modo irreversibile la relazione fra corpo e identità[1] e la crescente diffusione di un loro mercato, hanno sollevato una serie di questioni essenziali sia da un punto di vista etico che giuridico, considerando la possibile fallibilità di questi sistemi, gli errori algoritmici frequenti nel riconoscimento, le gravissime conseguenze in caso di furto d'identità e l'attitudine del dato biometrico a rilevare ulteriori informazioni sensibili rispetto alla finalità identificativa quali la salute, il sesso, l'etnia e altre informazioni sensibili deducibili da essi[2]. Altri aspetti critici legati all'uso dei sistemi biometrici concernono la capacità di queste tecnologie di raccogliere efficacemente informazioni a distanza o in movimento, anche all'insaputa dell'individuo, nonché le tecniche di profilazione e sorveglianza che possono derivare dall'elaborazione di questi dati. Connesso a quest'ultimo aspetto vi è anche il rischio legato a un uso indebito di questi dati per finalità ulteriori rispetto a quelle della loro raccolta, difficile se non quasi impossibile da scoprire per un individuo. Pertanto, una diffusione incontrollata del ricorso alla

[1] Garante Europeo della Protezione dei Dati, *Parere sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata*, in G.U.C.E. 23 luglio 2005, n. C 181.

[2] Discorso del professor Rodotà di presentazione della Relazione per l'anno 2001, Garante per la protezione dei dati.

biometria oltre a situazioni di stretta necessità rischia di limitare fortemente la percezione nella nostra società delle minacce poste da questi sistemi alla tutela della nostra privacy. La biometria[3], dunque, solleva numerose questioni che fin da subito hanno costituito un oggetto d'attenzione per policy makers e studiosi internazionali del settore. Lo scopo del presente contribuito pertanto è quello di delineare le questioni giuridiche legate al trattamento dei dati biometrici, ponendo un confronto in chiave comparata fra la disciplina biometrica dell'ordinamento europeo e la disciplina biometrica dell'ordinamento statunitense, a partire dalla loro emersione fino alle innovazioni più recenti.

Prioritariamente, però, per comprendere il dato giuridico è necessario ripercorrere alcuni aspetti tecnici essenziali legati al funzionamento di questi sistemi biometrici. Il riconoscimento biometrico si fonda su tecniche di analisi quantitativa di caratteristiche fisiche, fisiologiche o comportamentali finalizzate al riconoscimento univoco di un soggetto. Tecnologie biometriche sempre più avanzate consentono infatti di disporre il riconoscimento di un individuo a partire da un suo attributo distintivo misurabile quantitativamente, come un'impronta digitale, la fisionomia del volto, l'iride e la retina, la geometria della mano, la voce e il movimento labiale, l'andatura e la firma. Si tratta di un fenomeno talmente dinamico e soggetto a innovazioni, che non è possibile elencare in modo onnicomprensivo ogni tipologia di rilevazione biometrica.

In relazione ai dati biometrici, tuttavia, è possibile individuare alcune caratteristiche essenziali comuni ad ognuno di essi. Ogni dato biometrico risulta infatti quantitativamente misurabile, universale in quanto presente in ogni persona, unico poiché riferibile ad un solo individuo e permanente, poiché generalmente immutabile nel tempo[4]. Orientativamente, si tende a effettuare una distinzione fra caratteri biometrici forti, deboli e tenui, dove i primi riguardano caratteri del tutto immutabili come la scansione dell'iride o le impronte digitali, i secondi si riferiscono a caratteristiche che possono variare nel tempo come la voce, l'odore o l'andatura di una persona e gli ultimi riguardano caratteri generici come l'età, il sesso o il colore dei capelli[5]. Tuttavia a livello classificatorio i dati biometrici possono distinguersi essenzialmente solo all'interno di due macro categorie: i dati relativi a misure di caratteri fisici o fisiologici e i dati che rilevano fattori psicologici o comportamentali (come l'andatura, il timbro della voce o il modo di apporre una firma). I sistemi biometrici posso dunque utilizzare uno di questi elementi o rifarsi a una sola di queste categorie, anche se nella maggior parte dei casi si fondano su modelli ibridi basati su una combinazione di queste tecniche. Fondamentalmente, possiamo stabilire che il processo di riconoscimento biometrico

[3] Il termine biometria deriva dal greco βίος "vita" e μέτρον "misura", con cui si designa l'esposizione sistematica delle indagini quantitative intorno ai fenomeni della vita.

[4] Garante per la protezione dei dati personali, *Linee guida in materia di riconoscimento biometrico e firma grafometrica*, Allegato A al provvedimento del Garante del 12 novembre 2014 (doc. web. 3563006).

[5] A. K. Jain, P. Flynn, A. A. Ross, *Handbook of biometrics*, Springer, 2007, p. 1-4.

si articoli in tre fasi: attraverso la rilevazione, la conservazione e il confronto del dato[6]. Nella prima fase i caratteri biometrici vengono rilevati attraverso un dispositivo che estrae il carattere in questione, traducendolo in un formato digitale. Dopo la rilevazione, il campione biometrico così ottenuto può essere ulteriormente elaborato per determinarne un modello biometrico, che possa essere confrontato con altri modelli salvati in precedenza. Per semplificare questa parte, ad esempio, l'immagine di un volto costituisce il campione biometrico dal quale è possibile estrarre ulteriori tratti biometrici, come la geometria del volto. Il modello biometrico viene successivamente registrato e conservato all'interno di una banca dati a livello centralizzato, oppure a livello decentralizzato direttamente su un dispositivo elettronico in possesso dell'utente. Nell'ultima fase, invece, si dispone il confronto fra il modello biometrico registrato e quello acquisito dal sistema in tempo reale al fine di identificare il soggetto in questione. Questi sistemi biometrici non sono tuttavia a prova di errori e possono dar luogo sia a falsi match positivi che negativi. Inoltre, i caratteri biometrici possono non essere unici o permanenti e possono subire delle alterazioni a causa di un malfunzionamento del sistema o di fattori ambientali. Dopo aver riassunto brevemente gli aspetti tecnici essenziali legati al funzionamento sistemi di riconoscimento biometrico, possiamo addentrarci nel loro inquadramento in ambito giuridico. Alla base del successo delle tecniche di riconoscimento biometrico e del loro utilizzo su larga scala vi sono l'unicità, l'universalità e l'usabilità di questi sistemi.

Per tracciare l'evoluzione della disciplina in materia di biometria all'interno dell'ordinamento europeo e statunitense, è necessario sottolineare la forte interdipendenza con la tutela della privacy. Se, da un lato, infatti, l'adozione di tecnologie basate sulla biometria è spesso incoraggiata per migliorare la sicurezza dei sistemi informatici, dall'altro, il loro utilizzo e i margini di errore ad esse connessi possono avere conseguenze molto impattanti sulle vite delle persone. I sistemi biometrici hanno campi di sviluppo e applicazione ampi e variegati. Da un lato, il loro enorme potenziale ha attirato gli investimenti di privati e grandi aziende, che hanno utilizzato i dati biometrici per garantire l'accesso ai servizi, l'attivazione di dispositivi elettronici e lo sviluppo di sistemi di intelligenza artificiale per fini commerciali. Inoltre, in alcuni paesi, la biometria è stata ipotizzata per combattere l'assenteismo e controllare l'accesso dei dipendenti sul posto di lavoro. Anche nel settore pubblico, queste tecnologie stanno giocando un ruolo sempre più importante. Attualmente, il riconoscimento biometrico viene utilizzato in misure per migliorare la sicurezza pubblica o nazionale, facilitare lo sviluppo di indagini criminali, controllare le frontiere, prevenire azioni terroristiche e implementare l'efficienza di molti servizi pubblici. Tuttavia, il costante sviluppo e la commercializzazione di questi sistemi di determinazione biometrica all'interno di diversi settori può rivelarsi altamente insidioso e comportare molti rischi legati allo sfruttamento di questi sistemi, soprattutto per quanto riguarda il

[6] Ibidem.

rispetto dei diritti e delle libertà fondamentali dei suoi utenti. Inoltre, la ricerca nello sviluppo di questo settore è condotta prevalentemente da grandi multinazionali del digitale che detengono il capitale economico necessario per commercializzare questi sistemi nel mercato globale.

Queste multinazionali hanno acquisito ormai un patrimonio conoscitivo su questi sistemi per lo più irraggiungibile per le autorità pubbliche. Queste ultime, infatti, hanno avuto invece un approccio tardivo alla biometria, riconoscendo i rischi connessi all'uso di questi sistemi solo quando la loro diffusione era già ben avviata e difficile da limitare. Di fronte a una domanda di mercato in rapida crescita e al vuoto normativo prodotto dall'indecisione legislativa, questi attori economici si trovano spesso ad assumere anche un ruolo decisionale, tracciando autonomamente i propri limiti. Pertanto, si determina un contesto ibrido in cui mentre le autorità pubbliche tardano nel regolare accuratamente questo settore, le aziende private invece determinano le condizioni con cui disporre il commercio di queste tecnologie. Inoltre frequentemente il settore pubblico, che sta aumentando esponenzialmente l'uso della biometria in strategie di sicurezza pubblica, per farne utilizzo deve necessariamente dipendere da operatori privati. Gli operatori economici che regolano il commercio di questi sistemi in termini monopolistici sono anche in possesso di una risorsa cognitiva senza precedenti, come risultato dello sviluppo di tecnologie in grado di raccogliere passivamente i dati e determinarne informazioni altamente accurate sulle abitudini, i movimenti e l'identità degli utenti interessati. Attualmente, le aziende private possono scegliere se concedere a istituzioni ed enti pubblici l'acquisto di questi sistemi e quali informazioni condividere con loro.

Quindi, oltre ad avere un peso economico decisivo, questi giganti digitali possono condizionare ampiamente le autorità pubbliche, limitando il loro accesso a queste tecnologie, indirizzando la loro regolamentazione, intervenendo sulle forme di garanzia dei diritti fondamentali, e proteggendo libertà essenziali come la libertà di espressione. Situazioni di questo tipo testimoniano i forti rischi connessi all'uso di queste tecnologie e dovrebbero farci riflettere sulla reale necessità di una loro applicazione massiccia a fronte di rischi così elevati per i diritti della privacy, la libertà di espressione e la garanzia del principio di non discriminazione. Pertanto, nei prossimi capitoli ognuno di questi temi sarà approfondito in dettaglio attraverso il confronto fra la disciplina europea e la disciplina statunitense. Nel primo capitolo sarà affrontata la regolazione dei sistemi biometrici all'interno del diritto europeo, ripercorrendo la genesi del dibattito giuridico europeo in materia di biometria e le tappe definitorie del concetto di dato biometrico. In seguito, saranno approfonditi i dati biometrici inquadrati all'interno della prospettiva del Regolamento generale per la protezione dei dati personali (GDPR), analizzandone contestualmente alcuni elementi di criticità e i rischi posti alla tutela di alcuni diritti fondamentali. Da ultimo, saranno analizzate in dettaglio le tipologie di trattamento di dati biometrici attualmente riconosciute dal diritto europeo. Nel secondo capitolo, invece, sarà approfondita in

dettaglio l'esperienza italiana nella regolazione di questi sistemi, per mettere a fuoco la disciplina di uno stato membro rispetto all'implementazione delle disposizioni del GDPR e l'elaborazione di una propria disciplina autonoma. A partire dall'evoluzione del dibattito italiano sui dati biometrici, saranno discusse le innovazioni apportate dal decreto legislativo di recepimento delle disposizioni europee e il ruolo fondamentale giocato dal Garante italiano per la protezione dei dati personali nella regolazione di questo settore. Da ultimo, anche in questo caso, sarà disposta un'analisi dettagliata delle tipologie di trattamento di dati biometrici attualmente applicate nel nostro paese.

Infine, il terzo capitolo sarà incentrato sull'analisi della regolazione dei sistemi biometrici all'interno dell'ordinamento statunitense, ripercorrendo la genesi di questi sistemi legati allo sviluppo di importanti multinazionali del digitale e l'attuale stato della loro regolazione sia a livello nazionale che federale. Al momento negli Stati Uniti non è stata ancora implementata una legislazione federale legata al trattamento di dati biometrici, pertanto la sua disciplina giuridica sarà ricostruita attraverso l'esperienza di alcune leggi nazionali adottate in materia di biometria dagli stati del Texas, Illinois e Washington. Inoltre, attraverso del *Biometrics Information Privacy Act* dell'Illinois saranno discussi alcuni casi giurisprudenziali legati alla sua applicazione. Da ultimo, saranno approfonditi la necessità di adottare uno standard federale per la protezione dei dati biometrici e la possibilità di implementarlo adottando alcuni principi posti dalla disciplina europea del GDPR. Tale analisi permetterà di individuare elementi di pregio e difetti di entrambi i modelli di regolazione europeo e statunitense, e di ipotizzare una loro possibile convergenza verso una disciplina più trasversale con regole condivise per facilitare e rendere più sicuro l'uso di tali sistemi all'interno di un mercato digitale sempre più globale e interconnesso.

CAPITOLO 1: I DATI BIOMETRICI NELL'ORDINAMENTO EUROPEO

"*Si dà così rilevanza, in modo nuovo, al corpo, che diventa fonte diretta di informazioni, oggetto di un continuo "data mining", davvero una miniera a cielo aperto dalla quale attingere dati ininterrottamente. Lo ripetiamo: il corpo in sé sta diventando una password. La fisicità prende il posto delle astratte parole chiave, sostituite da impronte digitali, geometria della mano o delle dita o dell'orecchio, iride, retina, tratti del volto, odori, voce, firma, uso di una tastiera, andatura, Dna.*[7]*"*

(Stefano Rodotà, 2003)

1. L'evoluzione del dibattito europeo sui dati biometrici

L'avvento dell'uso della biometria e delle tecnologie ad essa connessa, ha accompagnato nuove riflessioni sul nostro concetto di identità e sulle libertà dei nostri corpi, come ci ricordano le parole del professor Rodotà in un intervento risalente al 2003. Nonostante vi siano testimonianze storiche risalenti in merito all'adozione di forme di riconoscimento fondate su dati biometrici[8], è solo a partire dall'ultimo secolo e ancora maggiormente in quello attuale, che grazie al progresso tecnologico l'utilizzo di questa nuova forma di determinazione dell'identità ha conosciuto la sua massima espansione, trovando numerosi ambiti di applicazione e una grande varietà di scopi. Alla base del successo delle tecniche di riconoscimento biometrico e del loro impiego in larga scala vi sono l'unicità, l'universalità, nonché la facile "catturabilità" e la permanenza di questa tipologia di dati, tali da far sì che i nostri corpi si siano trasformati in delle vere e proprie chiavi di accesso, delle *password* di riconoscimento[9].

[7] Discorso di presentazione della Relazione 2003, a cura di Stefano Rodotà Presidente dell'Autorità Garante per la Protezione dei Dati.

[8] Come illustrato dal lavoro storico di E.J. Kindt, si hanno riprove di questo tipo di forme di riconoscimento grazie alle impronte di mani nelle pitture rupestri paleolitiche, all'utilizzo delle impronte digitali per stringere patti commerciali nell'antica Babilonia, nella Cina della dinastia Tang, fino alla nascita dell'antropometria giudiziaria nella Francia di fine Ottocento: Kindt E.J., *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, Dordrecht-Heidelberg-New York-Londra, 2013, 15, ss.

[9] G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *DPCE online* 2/2019, p. 1108.

Tracciando l'evoluzione della disciplina dei dati biometrici nel diritto europeo è necessario sottolineare la sua interdipendenza con la disciplina per la tutela della privacy: se da un lato l'adozione di tecnologie fondate sulla biometria viene spesso incoraggiata per migliorare la sicurezza dei sistemi informatici, in quanto ritenute delle *privacy enhancing technologies (PET)*, dall'altro il loro utilizzo e i margini di errori ad esse collegate possono avere conseguenze molto impattati sulla vita dell'individuo. Sebbene fosse assai rilevante nel dibattito giuridico già da fine Novecento, il dato biometrico fino all'introduzione del Regolamento UE n. 679/2016 (GDPR) ha sempre costituito un oggetto *sui generis*, evocato nelle riflessioni in dottrina, ma mai espressamente definito.

Ciò ha comportato una sua emersione in alcuni ambiti settoriali, quali quello della videosorveglianza o dell'autenticazione elettronica, ma mancando di una disciplina autonoma, fino alle innovazioni del GDPR il dato biometrico ha unicamente attirato a sé, inizialmente, la disciplina generale prevista per il dato personale ed in seguito la disciplina posta a tutela del dato sensibile[10]. Di fatto, non vi è alcuna menzione esplicita dei dati biometrici nei fondamenti della disciplina sulla protezione dei dati personali, quali l'art. 8 CEDU, la Convenzione 108/1981[11] nella sua stesura originaria, gli artt. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea, la direttiva 95/46/CE[12] e la direttiva 2002/58/CE[13]. All'epoca la diffusione delle tecnologie biometriche era certamente ancora agli albori, ma questo non implicava che i dati biometrici fossero estranei al dibattito giuridico.

Nell'aprire il dibattito sulla loro regolazione, un ruolo fondamentale è stato ricoperto dal Gruppo di lavoro per la protezione dei dati personali (WP29), istituito dalle previsioni dell'art. 29 della direttiva 95/46/CE. Questo soggetto rivestiva il ruolo di organismo consultivo e indipendente dell'Unione Europea per la protezione dei dati personali e del diritto alla riservatezza. I suoi compiti erano regolati dall'art. 30 della direttiva 95/46/CE e dall'art. 15 della direttiva 2002/58/CE e il WP29 operava come il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati interne alla comunità europea[14]. Il Documento di lavoro sulla biometria del 2003[15], elaborato sotto la presidenza di Rodotà durante le attività del WP29, costituisce ancora oggi il primo tassello essenziale per ricostruire lo stato della disciplina europea in materia di dati biometrici. Il Documento di lavoro si prefiggeva l'obiettivo di garantire un'applicazione omogenea delle disposizioni nazionali in materia

[10]R. Ducato, *I dati biometrici*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, G. Giappichelli Editore, 2019, p. 1295.

[11] Convenzione di Strasburgo n. 108/1981 legge 21 febbraio 1989, n. 98.

[12] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in G.U.C.E 23 novembre 1995, n. l. 281/31.

[13] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, in G.U.C.E 31 luglio 2002, n. l. 201/37.

[14] Dalla pagina ufficiale dedicata all'*Article 29 Working Party* sul sito della Commissione Europea. https://ec.europa.eu/newsroom/article29/items/itemType/1358

[15] Gruppo Art. 29, Documento di lavoro sulla biometria, adottato il 1° agosto 2003, 12168/02/IT WP 80.

di protezione dei dati, conformemente alla direttiva 95/46/CE, in relazione ai sistemi biometrici[8]. In esso, inoltre, emergeva per la prima volta una descrizione dei sistemi biometrici, intesi come "le applicazioni di tecnologie biometriche che permettono l'identificazione e/o l'autenticazione/verifica automatica di un individuo[8]". Sebbene non si trattasse di una vera e propria definizione giuridica del dato biometrico, il WP29 aveva studiato nel dettaglio il funzionamento delle tecnologie applicabili alla biometria, definendo i primi contorni della sua disciplina attraverso i principi della direttiva 95/46/CE. Sulla base dell'art. 2, lett. a) della suddetta, "i dati biometrici possono sempre essere considerati come "informazione concernente una persona fisica" in quanto sono dati che, per la loro stessa natura, forniscono informazioni su una determinata persona[8]". Pertanto, la disciplina e i principi generali attribuiti alla tutela del dato personale dovevano essere estesi integralmente anche al dato biometrico. Secondo il parere del WP29 l'impiego delle tecniche biometriche era da intendersi ammissibile solo se realmente proporzionato agli scopi, escludendo però la creazione di archivi centralizzati e l'utilizzazione di informazioni desunte da tracce fisiche, come le impronte digitali, che possono essere rilevate da una persona anche senza la sua volontà[16].

A partire da queste considerazioni il Gruppo ha voluto tracciare un quadro di riferimento che fosse omogeneo nella sua applicazione europea, sia per l'industria di tali sistemi biometrici che per la tutela dei singoli utenti. A tal fine veniva ribadita l'esigenza di identificare con chiarezza le finalità del ricorso a sistemi biometrici, sulla base del principio di necessità, verificando se lo scopo perseguito potesse essere raggiunto egualmente mediante strumenti meno invasivi. Nelle parole di Rodotà, "il principio di necessità impone di accertare se la finalità perseguita non possa essere realizzata utilizzando dati che non coinvolgano il corpo".

Questo principio orientava anche la preferenza, da parte dei Garanti nazionali, per i dati biometrici che potessero essere memorizzati attraverso dei dispositivi periferici (*smartcard*, tessera magnetica), riducendo i rischi a cui i soggetti sarebbero stati esposti nel caso di archivi centralizzati. Inoltre, nel Documento di lavoro veniva espressamente sancito il divieto di impiegare dati biometrici per finalità contrarie a quelle con cui sono stati raccolti e l'obbligo di informazione degli interessati. Nel caso in cui fossero applicati sistemi di memorizzazione centralizzati veniva imposto un controllo preliminare ai sensi dell'art. 20 della direttiva 95/46/CE; in quanto il principio di proporzionalità imponeva una ponderazione adeguata della legittimità di raccolte generalizzate, rispetto a raccolte mirate.

Incalzato dagli innovativi avanzamenti nel settore, il WP29 tornò ad occuparsi dei progressi nell'industria della biometria un decennio dopo, attraverso il Parere n. 3/2012 sugli sviluppi nelle

[16] Nota introduttiva nella pagina web introduttiva al Documento di lavoro sulla biometria 2003, sul sito ufficiale del Garante per la protezione dei dati personali. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1609419

tecnologie biometriche[17]. In esso si ribadiva il ruolo centrale della biometria nella scienza forense e nei sistemi di controllo dell'accesso in grado di aumentare i livelli di sicurezza, rendendo le procedure di identificazione rapide e agevoli. I notevoli traguardi raggiunti negli ultimi anni, però, evidenziavano minacce concrete per i diritti fondamentali dei cittadini, dal rischio di subire una discriminazione genetica al furto della propria identità[18].

Il Parere n. 3/2012 aveva l'obiettivo di tracciare un quadro chiaro delle opportunità e dei rischi connessi allo sviluppo di queste nuove tecnologie e al loro impiego sia nel settore pubblico, che nel settore privato. I dati biometrici sono per propria natura destinatari di un legame diretto con un soggetto specifico, che non può essere spezzato, pertanto pongono i legislatori europei di fronte a nuove criticità: se da un lato queste tecnologie spesso vengono celebrate come innovazioni in grado di migliorare l'esperienza dell'utente e la fruibilità dei servizi, in assenza di forme di garanzia adeguate può essere seriamente pregiudicato il diritto alla riservatezza degli utenti interessati.

Dunque, attraverso le attività del WP29 venivano delineate apposite misure tecniche e organizzative per attenuare i rischi per la protezione dei dati e la vita privata, che potessero in qualche modo minare alla tutela di questi diritti fondamentali. Le tecnologie biometriche sono strettamente connesse a caratteristiche dell'individuo, che possono rivelare informazioni sensibili a livello genetico o sul suo stato di salute. Molti di questi sistemi consentono il tracciamento automatizzato o la localizzazione degli utenti, nonché misure di profilazione strategiche a livello commerciale, per questo il loro impatto potenziale sulla vita privata dei cittadini europei è estremamente elevato ed è direttamente proporzionale all'esponenziale aumento nella diffusione di questi sistemi biometrici.

In particolare, veniva posto un accento specifico sullo sviluppo di tecnologie inerenti al riconoscimento facciale nell'ambito dei servizi online o mobili, su cui era stato redatto un apposito parere nel medesimo anno. Sulla base del Parere 2/2012[19], queste tecniche consentono di riprendere le immagini di una persona, anche senza che essa ne sia consapevole, trasmettendole poi a server remoti ai fini di ulteriore trattamento. Ciò ha permesso a numerose imprese private, gestori di servizi online, di acquisire ampie raccolte di immagini caricate online dagli stessi interessati.

In certi casi queste informazioni possono anche essere raccolte illegalmente rastrellando siti pubblici o motori di ricerca. Inoltre, i nuovi *smartphone* dotati di piccole fotocamere ad alta risoluzione avevano reso possibile per chiunque trasmettere immagini in tempo reale, anche senza il consenso dei diretti interessati. Gli scenari aperti dallo sviluppo di queste tecnologie, sempre più fruibili nel

[17] Gruppo Art. 29, Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, adottato il 27 aprile 2012, 00720/12/IT WP193.
[18] T. B. Gillis, J. L. Spiess, *Big Data and Discrimination*, in *The University of Chicago Law Review*, Vol. 86, No. 2, 2019, p. 460-463.
[19] Gruppo Art. 29, Parere 2/2012 relativo al riconoscimento facciale nell'ambito dei servizi online e mobili, adottato il 22 marzo 2012, WP192.

nostro quotidiano, ponevano quindi l'esigenza di un'attenzione specifica da parte del WP29 nell'adeguamento delle misure a garanzia della protezione dei dati[20]. Questi pareri rivolti all'autorità europea e alle autorità nazionali di regolamentazione, nonché ai responsabili del trattamento dei dati e gli utilizzatori di tali tecnologie, miravano dunque a esaminare il quadro giuridico europeo e formulare delle apposite raccomandazioni da adottare nell'impiego di queste tecnologie biometriche. Sebbene all'epoca fosse ancora assente una disciplina specifica per il trattamento dei dati biometrici e a livello europeo fosse prevista solo l'estensione al dato biometrico della disciplina posta dalla direttiva 95/46/CE sul dato personale, nell'arricchire il dibattito in dottrina sugli sviluppi della biometria si rese determinante anche l'attività del Consiglio d'Europa.

Come sostenuto inizialmente, la Convenzione 108/1981, nota come la Convenzione di Strasburgo, non conteneva alcun riferimento esplicito ai dati biometrici nella sua stesura originale. Essa però al contempo risulta essenziale in quanto costituisce uno dei più importanti strumenti legali per la tutela della protezione dei dati personali dei cittadini europei e rappresenta l'unico strumento giuridicamente vincolante a livello internazionale.

Infatti, ad essa possono aderire anche stati non appartenenti all'Unione Europea. La Convenzione si applica a tutti i trattamenti di dati personali che siano effettuati sia nel settore privato, che nel settore pubblico, comprese le autorità giudiziarie e di polizia. Tramite questa normativa negli anni si è cercato di implementare le tutele degli individui contro possibili abusi, provvedendo a dare una disciplina unica ai flussi transnazionali di dati[21].

Negli anni successivi però il Consiglio d'Europa ha progressivamente tracciato le questioni giuridiche salienti e fornito le prime indicazioni per delineare la disciplina del trattamento dei dati biometrici in linea con le previsioni della Convenzione, a partire dalla pubblicazione del *Progress Report 2005*[22].

La relazione del Consiglio d'Europa costituiva l'esito del lavoro avviato nel 2003 dal Project Group on Data Protection (CJ-PD) sotto la guida dell'European Committee on Legal Cooperation (CDCJ) e del Comitato consultivo della Convenzione per la protezione delle persone rispetto al trattamento automatizzato dei dati personali[23]. La prefazione della relazione sullo stato di avanzamento del 2005 affermava la necessità di adottare una posizione sull'applicazione della protezione dei dati alla biometria con urgenza, al fine di contribuire al dibattito in corso e ai progetti di regolazione già avviati

[20] C. Jasserand, *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, in *European Data Protection Law Review (EDPL)* n. 297, 2016, 2(3), p. 300-301.

[21] Dal sito ufficiale del Consiglio d'Europa: https://www.coe.int/it/web/conventions/full-list?module=treaty-detail&treatynum=108

[22] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* ('Progress Report 2005'), Strasbourg 2005.

[23] P. Hert, K. Christianen, *Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric data*, Tilburg University, 2013, p. 5-6.

sia a livello nazionale che europeo. Per questo, all'interno del *Progress Ropert 2005* erano inserite 12 raccomandazioni, che dovevano orientare l'attività dei legislatori europei.
In seguito al protocollo adottato nel 2005, negli anni successivi continuò ad accrescersi il dibattito attorno all'ideazione di un protocollo di aggiornamento della Convenzione 108/1981 che nella sua versione c.d. "modernizzata", desse un riconoscimento effettivo anche al dato biometrico.
La modernizzazione della Convenzione 108 perseguiva due obiettivi principali: affrontare le sfide derivanti dall'uso delle nuove tecnologie dell'informazione e della comunicazione e rafforzare l'effettiva attuazione della Convenzione. I lavori per la stesura del protocollo di aggiornamento procedevano sotto la guida del Committee on Data protection (CAHDATA). Nel 2014 venne trasmessa la prima stesura dell'emendamento alla Convenzione, diffusa attraverso il *Draft Explenatory Report*[24], mentre la versione consolidata della Convenzione 108/1981 venne emanata solo nel settembre 2016, seguita dalla pubblicazione della versione definitiva dell'*Explenatory Report to the Protocol amending the Convention*[25], che già teneva conto delle innovazioni apportate alla materia dalla recente introduzione del nuovo GDPR. Nella versione "modernizzata" della Convenzione si apportava una sostanziale modifica all'art. 6, inserendo esplicitamente i dati biometrici come categoria speciale di dati.
Secondo il testo dell'articolo:

a) The processing of: genetic data, personal data relating to offences, criminal proceedings and convictions, and related security measures; *biometric data uniquely identifying a person*; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life;

   shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.

b) Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

Pertanto, non solo si aveva il primo riconoscimento formale del dato biometrico, ma anche la sua caratterizzazione come categoria di dato sensibile, al quale dovevano essere accordate delle forme

[24] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Draft Explanatory report of the modernized version of Convention 108*, 2014.
[25] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 10 Settembre 2018.

di garanzia speciali. Il catalogo dei dati sensibili era stato ampliato dunque per includere i dati genetici e biometrici, nonché i dati trattati per le informazioni da essi rilevabili relative all'appartenenza sindacale o all'origine etnica[26]. Inoltre, nel commento all'art. 6 riportato nell'*Explenatory Report* i dati biometrici sono identificati come "data resulting from a specific technical processing of data concerning the physical, biological, or physiological characteristics of an individual which allows the unique identification or authentication of the individual". L'Italia ha sottoscritto il Protocollo emendativo della Convezione 108/1981 il 5 maggio 2019.

1.1 Le tappe definitorie del concetto di dato biometrico

Prima di addentrarci nell'analisi delle innovazioni apportate dall'introduzione del GDPR, è necessario ancora soffermarci su un aspetto essenziale relativo al quadro delineato con la presente analisi: la definizione di dato biometrico è un'innovazione giuridica introdotta a livello europeo con l'adozione del GDPR, prima di allora la nozione di dato biometrico era ricavata prevalentemente a livello interpretativo in dottrina[27]. Abbiamo già analizzato, infatti, alcuni tentativi definitori da parte del WP29 e del Comitato consultivo per la Convenzione 108. Già nel Documento di lavoro sulla biometria del 2003, pur in assenza di una definizione formale, si era ricondotta la natura giuridica del dato biometrico alla categoria generale del dato personale.

Il primo vero intento definitorio però deve essere ricondotto ad un altro intervento del WP29, ossia il Parere 4/2007[28], nel quale i dati biometrici vengono descritti come "proprietà biologiche, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche e/o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità"[23].

Si identifica, dunque, il dato biometrico sotto una duplice natura, in quanto le informazioni ricavabili da un dato biometrico sono in primis attribuibili al soggetto a cui si riferiscono (es. un soggetto ha questa struttura della retina o del volto), ma possono essere anche strumentali all'applicazione di tecniche di riconoscimento (es. la struttura della retina rilevata corrisponde a quella precedentemente memorizzata del soggetto in questione). Il dato biometrico può pertanto essere ritenuto dato personale sia in riferimento alla sua natura, sia come identificatore unico e inalterabile di un soggetto[29].

[26] Queste ultime due categorie si aggiungevano al già vigente divieto di trattamento dei dati personali che rilevassero l'origine razziale, opinioni politiche o convinzioni religiose o di altro genere, salute o vita sessuale e dati personali relativi a reati, procedimenti penali e condanne.

[27] R. Ducato, *I dati biometrici*, cit., p. 1301.

[28] Gruppo Art. 29, Parere 4/2007 sul concetto di dati personali, adottato il 20 giugno 2007, 01248/07/IT WP136.

[29] C. Jasserand, *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, in *European Data Protection Law Review (EDPL)* n. 297, 2016, 2(3), p. 300-303.

Come descritto in dottrina, la definizione riportata nel Parere 4/2007 [30] è stata adottata anche nei pareri emanati dal Garante Europeo della Protezione dei Dati (EDPS) concernenti la materia. In alcuni pareri[31] dell'EDPS ci si focalizza, inoltre, sul carattere "sensibile" dei dati biometrici e sui rischi connessi al loro tracciamento e alla fallibilità di questi sistemi.

Nella ricostruzione del retroterra giuridico europeo in materia di biometria, non è secondaria di fatto l'analisi dei rischi connessi all'uso di queste tecnologie: i dati biometrici rendono processabili tratti corporei che una volta acquisiti diventano identificabili e leggibili in modo ripetitivo. Questa tipologia di dati ha la naturale tendenza a lasciare sue tracce nell'ambiente, che possono essere rilevate anche senza il consenso dell'interessato. Inoltre, queste tecnologie presentano un significativo livello di fallibilità nelle loro procedure di analisi e identificazione, per questo spesso si identificano come metodi che "comportano un certo grado di probabilità". Altra questione spinosa è quella relativa al furto di identità: essendo il dato biometrico per sua natura quasi immutabile, un furto, ad esempio, di dati biometrici relativi al riconoscimento facciale di un soggetto può pregiudicare enormemente la sua privacy e la sua sicurezza, essendo questi tratti impossibili da modificare una volta sottratti illegalmente[32]. Infine, l'ultimo tassello già analizzato concerne l'art. 6 della Convenzione 108 modernizzata, nel quale il dato biometrico viene inquadrato all'interno della categoria del dato sensibile. Questi primi tentativi definitori sono estremamente significati ai fini di questa ricerca, in quanto delineano l'impianto normativo su cui poi si innesterà concretamente la successiva riforma in materia dei dati personali del 2016. Come vedremo nei successivi paragrafi, è solo con la proposta della Commissione del 2012 che i dati biometrici otterranno riconoscimento all'interno di un testo destinato ad avere una forza cogente all'interno dei sistemi giuridici nazionali degli Stati membri. L'analisi dell'evoluzione del concetto di dato biometrico di fatto non costituisce un esercizio fine a sé stesso, ma un procedimento essenziale per tracciare l'ambito di applicazione della sua disciplina. In particolare, vi sono alcuni aspetti comuni che emergono dalle attività di WP29, EDPS e Comitato consultivo per la Convenzione 108, che possiamo distinguere fin da adesso[33]:

- La disciplina generale relativa alla protezione dei dati personali viene estesa integralmente alla tutela dei dati biometrici, pertanto il dato biometrico appartiene alla categoria di dato personale

[30] R. Ducato, *I dati biometrici*, cit., p. 1303.

[31] Garante Europeo della Protezione dei Dati, *Parere sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata* (COM(2004) 835 definitivo).

ID., *Opionion on a notification forr prior cheching received from the Data Protection Officer (DPO) of the European Parliament in connection with the "Biometric verification device" case,* 15 maggio 2014.

[32] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, in *20 J. High Tech*, l. 229, 2020, p. 267-269.

[33] R. Ducato, *I dati biometrici*, cit., p. 1304-5.

- Si può trattare di dato biometrico solo in presenza di un apposito sistema che ne predisponga la sua elaborazione e utilizzo per una finalità identificativa/di verifica; se il dato non viene rilevato a fini di identificazione o autenticazione di un individuo, non è da intendersi "biometrico" in senso giuridico
- Se il trattamento del dato biometrico concerne fini identificatori[34], considerati i rischi elevati connessi al trattamento dei dati biometrici, viene giustificato il loro inquadramento all'interno della categoria più ristretta dei dati sensibili
- Infine, nessuno di questi intenti definitori descrive e analizza nello specifico le modalità di trattamento dei dati biometrici

Una volta circoscritti questi primi elementi, possiamo adesso addentrarci nel dibattito giuridico alla base della riforma in materia di dati personali del 2016.

2. I dati biometrici nella prospettiva del GDPR

Nel 2012 la Commissione europea presenta una proposta di riforma in materia di protezione dei dati, con l'obbiettivo di adeguare l'impianto normativo europeo alle nuove frontiere dell'era digitale. All'epoca oltre il 90% dei cittadini europei auspicava che i diritti e le garanzie per la tutela dei dati personali fossero le stesse in tutta l'Unione Europea, a prescindere dal luogo in cui fosse effettuato il trattamento dei dati[35]. Nella proposta di Regolamento generale sulla protezione dei dati[36], che avrebbe sostituito le disposizioni della direttiva 95/46/CE, per la prima volta si aveva una configurazione giuridica del dato biometrico, codificato all'interno dell'art. 4, dedicato alle definizioni.
Inoltre, il dato biometrico emergeva anche all'interno dell'art. 33 della proposta di Regolamento, fra le ipotesi di trattamento connesse a rischi specifici per i diritti e le libertà degli interessati. Questa prima manifestazione del dato biometrico all'interno del GDPR appariva però troppo coincisa. Nella definizione inserita all'interno della proposta, infatti, veniva esposto un generico riferimento a "qualsiasi dato", relativo alle caratteristiche fisiche, fisiologiche o comportamentali, senza mettere in relazione le modalità di ottenimento o di creazione dello stesso. Venivano menzionati solo i dati biometrici che consentissero operazioni di identificazione e non anche autenticazione. Da ultimo, i

[34] In realtà, secondo I pareri dell'EDPS i rischi connessi al trattamento dei dati biometrici giustificano un'estensione generale della nozione di dato sensibile all'intera categoria di dati biometrici, indipendentemente dalla condizione che il loro trattamento avvenga per fini identificatori.
[35] Commissione Europea, Comunicato Stampa 15 dicembre 2015 "*Protezione dei dati nell'UE: l'accordo sulla riforma proposta dalla Commissione stimolerà il mercato unico digitale*".
https://ec.europa.eu/commission/presscorner/detail/it/IP_15_6321
[36] Commissione Europea, "Proposta di Regolamento del Parlamento Europeo e del Consiglio, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati" (COM(2012) 11 final).

dati biometrici non erano inizialmente inclusi nelle categorie particolari di dati personali disciplinate dall'art. 9[37]. Nonostante ciò, i successivi passaggi legislativi contribuirono notevolmente allo sviluppo dell'inquadramento giuridico del dato biometrico.

Essenziale fu il contributo del Parlamento europeo, il quale in prima lettura rese esplicita la natura di dato personale del dato biometrico, attraverso una precisazione linguistica all'art. 4, modificando il riferimento generico a "qualsiasi dato". Inoltre, attraverso l'emendamento 1042 presentato dal parlamentare Dimitrios Droutsas, il Parlamento ha incluso esplicitamente il dato biometrico fra le categorie speciali di dati personali[38]. Il Consiglio dell'UE, nell'orientamento generale del Consiglio di Giustizia e Affari Interni pubblicato nel giugno 2015[39], si è espresso sulla definizione di dato biometrico. In particolare, secondo il suo orientamento tale definizione è applicabile solo ai dati personali che siano ottenuti tramite uno specifico procedimento tecnico, che renda possibile l'identificazione univoca di uno soggetto. Il Consiglio ha in seguito predisposto un *addendum* al testo della disposizione all'art. 9 dedicato alle categorie particolari di dati, prevedendo la possibilità per gli Stati membri di poter introdurre ulteriori limitazioni e previsioni in materia di dati biometrici. Infine, è stato predisposto anche un inciso relativo al caso specifico della fotografia, all'interno del *considerando 51*. Dopo gli interventi del Parlamento europeo e del Consiglio dell'UE, le modifiche apportate sono confluite nel testo finale del Regolamento UE n. 679/2016, pubblicato in Gazzetta Ufficiale europea il 4 maggio 2016 ed entrato in vigore il 24 maggio 2016 (anche se la sua attuazione è avvenuta solo a partire dal 25 maggio 2018).

All'art. 4, par. 14, GDPR pertanto troviamo la versione definitiva della definizione giuridica dei dati biometrici, descritti come "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici". Inoltre possiamo distinguere tre caratteri specifici dei dati biometrici: l'universalità, in quanto sono dati rinvenibili in ogni soggetto; l'esclusività, in quanto ogni dato biometrico è unico per ogni persona e la permanenza, poiché il dato biometrico resta immutato nel tempo, salvo casi eccezionali come traumi o lesioni[40].

[37] R. Ducato, *I dati biometrici*, cit., p. 1306.

[38] Risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati; Regolamento generale sulla protezione dei dati (COM (2012) 0011-C7-0025/2012-2012/0011 (COD).

[39] Consiglio dell'Unione europea, orientamento generale del Consiglio di Giustizia e Affari Interni 9565/15, 11 giugno 2015.
https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/it/pdf

[40] M. Soffientini, *Privacy, protezione e trattamento dei dati*, IPSOA Manuali, 2018, p. 276.

Questa definizione si ispira alla definizione tecnica postulata dallo standard ISO/IEC 2382-37, preferendo la nozione del termine "identificazione" a quella del termine "autenticazione"[41]. Inoltre, il *considerando 51* precisa che il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando sono trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica[42]. Una foto di amici scattata con il proprio telefono non può essere qualificata di fatto come un dato biometrico, a meno che essa non sia elaborata da sistemi che applichino forme di riconoscimento facciale. Anche nel caso dei dati dattiloscopici non rientrano nella definizione di dato biometrico le mere caratteristiche biometriche rilevate al loro stato naturale, ma solo i dati che, una volta sottoposti ad un procedimento tecnico, siano stati trasformati in campioni biometrici.

Il dato biometrico viene configurato come una categoria particolare di dato personale, esso infatti non concerne qualsiasi informazione relativa a una caratteristica fisica, fisiologica o comportamentale di un soggetto, ma solo quelle informazioni che vengono ricavate attraverso specifici procedimenti tecnici e che comportano l'identificazione univoca di un individuo[43]. Esso pertanto deve essere analizzato in relazione a due fattori: in primo luogo la dipendenza tecnica del dato dal sistema biometrico che ne consente la rilevazione[44], mentre in secondo luogo la finalità identificativa che è alla base del suo trattamento.

Oltre all'art. 4, par. 14, il GDPR menziona i dati biometrici anche all'interno dell'art. 9, dedicato al trattamento di categorie particolari di dati personali[45]. In esso nel primo paragrafo si sancisce il divieto di trattamento dei dati personali che possano rilevare aspetti sensibili della persona, quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, l'appartenenza sindacale, nonché i dati biometrici e genetici intesti a identificare in modo univoco una persona, dati sulla salute o sull'orientamento e vita sessuale. Dunque, il GDPR sancisce come regola generale il divieto di trattamento per queste categorie particolari di dati. Tuttavia, sono previste una serie di eccezioni elencate al secondo paragrafo del medesimo articolo, nel quale sono descritti in dettaglio i casi in cui le previsioni del primo paragrafo possono non applicarsi.

[41] ISO/IEC 2382-37 "Information Technology – Vocabulary – Part 37: Biometrics".
[42] Garante per la protezione dei dati personali, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, arricchito con riferimenti ai Considerando, p. 14-15.
[43] C. Jasserand, *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, cit., p. 301-304.
[44] I dati biometrici non sono entità autonomamente rilevabili nella realtà fenomenica, ma informazioni che sottoposte a processi di elaborazione tecnica.
[45] M. Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information*, in *University of Miami International and Comparative Law Review*, 2018, 25(2), p. 381-384.

Il primo caso (lett. a) concerne l'eventualità che l'interessato abbia prestato il proprio consenso esplicito al trattamento. Di fatto il trattamento dei dati sensibili può essere effettuato solo sulla base del consenso esplicito dell'interessato.
Oltre al consenso esplicito dell'interessato, il trattamento dei dati sensibili può avere luogo se:

b) è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
e) riguarda dati personali resi manifestamente pubblici dall'interessato;
f) è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
h) è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
i) è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e

specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Infine i paragrafi 3 e 4, consentono il trattamento ai sensi della lettera h) se tali dati sono trattati sotto la responsabilità di un professionista soggetto al segreto professionale o alle norme stabilite dagli organismi nazionali competenti e stabiliscono la possibilità per gli Stati membri di introdurre ulteriori condizioni, o limitazioni, con riguardo al trattamento di dati genetici, biometrici o relativi alla salute[46].
Nel dibattito legato alla genesi di questo articolo, la qualificazione del dato biometrico in termini di dato sensibile solleva qualche dubbio interpretativo. In particolare i dati biometrici sono l'unica categoria di dati inseriti all'interno del primo paragrafo accompagnati dalla precisazione della finalità del loro trattamento ("intesi a identificare in modo univoco una persona fisica")[47].
Esplicitando lo scopo del trattamento, il testo dell'art. 9 GDPR sembra escludere dal regime speciale previsto per i dati sensibili, i dati biometrici trattati per altre finalità quali la ricerca scientifica. Queste tipologie di dati biometrici possono dunque accedere al regime di protezione speciale solo se sono in grado di rilevare un'ulteriore categoria sensibile di dati personali, quali l'appartenenza etnica o lo stato di salute del soggetto (es. analisi del Dna). Quindi, stando a una lettura letterale delle previsioni del GDPR non tutti i dati biometrici sono dati sensibili in senso giuridico[48].
Un'altra questione riguarda invece la previsione alla lettera e), ossia il trattamento di dati sensibili resi manifestamente pubblici dall'interessato. Questa previsione può rivelarsi un'eccezione estremamente ampia al divieto di trattamento, specialmente alla luce delle recenti innovazioni tecnologiche e alla crescente pervasività dei *social network* nelle nostre vite.
È importante sottolineare però come essa non debba essere ritenuta alla stregua di un'autorizzazione indiscussa. Dopotutto, come vedremo nello specifico, per far sì che il trattamento sia lecito è necessario che ricorra una delle ipotesi definite dall'art. 6 GDPR, mentre l'art. 9, par. 2, lett. d) costituisce solo una condizione specifica che rende ammissibile il trattamento dei dati sensibili. Pertanto, affinché risulti lecito il trattamento di dati biometrici devono essere sempre valide e

[46] M. Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information,* cit., p. 392.
[47] R. Ducato, *I dati biometrici*, cit., p. 1311.
[48] C. Jasserand, *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, cit., p. 307-311.

verificabili le previsioni all'art. 9 e all'art. 6 GDPR. Definiti i contorni della natura giuridica dei dati biometrici, di seguito ci concentreremo in maggior dettaglio nell'analizzare le innovazioni apportate dal GDPR alla loro disciplina.

2.1 La disciplina del trattamento

Nel nuovo Regolamento sulla protezione dei dati sono state introdotte numerose disposizioni rilevanti per la disciplina del dato biometrico. In primo luogo, il trattamento dei dati biometrici deve essere ricompreso all'interno dell'ambito di applicazione del Regolamento, definito all'art. 2, par. 1, GDPR (che ricomprende anche il trattamento "interamente o parzialmente automatizzato di dati personali")[49] e all'art. 3 GDPR. L'art. 2 GDPR definisce l'ambito di applicazione materiale del GDPR, mentre l'art. 3 GDPR il suo ambito di applicazione territoriale. Quest'ultimo concerne il trattamento dei dati personali effettuati nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione (art. 3, par. 1 GDPR)[50].

Il trattamento di questa tipologia di dati deve essere inoltre conforme alle disposizioni espresse all'interno del Capo II, art. 5 GDPR, relativo ai principi applicabili al trattamento dei dati personali[51]. I principi di *liceità*, *correttezza* e *trasparenza*, stabiliscono che il trattamento sia conforme alla normativa generale, sia svolto in maniera leale ed onesta e che le informazioni e le comunicazioni relative al trattamento siano facilmente accessibili e comprensibili mediante un linguaggio semplice e chiaro[52]. Il principio di *limitazione della finalità*, esprime l'esigenza che i dati personali siano trattati secondo finalità determinate, esplicite e legittime. Il principio di *adeguatezza*, *pertinenza* e *non eccedenza*, stabilisce la necessità che i dati raccolti siano pertinenti e non superflui rispetto alla finalità dichiarata per il trattamento. Il principio di *esattezza* richiede un'attenta verifica dei dati, non solo al momento della loro raccolta ma anche nelle fasi successive attraverso periodici aggiornamenti.

[49] All'art. 2, par. 2, GDPR sono elencati i casi di esclusione del trattamento di dati personali dalla disciplina del GDPR; all'art. 2, par. 3, GDPR si stabilisce che per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il Regolamento (CE) n. 45/2001(che deve essere adeguato ai principi del presente Regolamento).
[50] L'art. 3, par. 2 GDPR stabilisce che il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
L'art. 3, par. 3 GDPR stabilisce che il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.
[51] M. Soffientini, *Privacy, protezione e trattamento dei dati*, cit. p. 93-96.
[52] *Considerando 39.*

Il principio di *limitazione della conservazione* esprime l'esigenza che la conservazione del dato avvenga attraverso modalità che consentano l'identificazione dell'interessato solo per il tempo necessario alla realizzazione della finalità perseguita. L'unica deroga ammissibile concerne l'archiviazione per ragioni di pubblico interesse, ricerca scientifica o storica o per ricerca statistica. Infine, i principi di *integrità* e *riservatezza* impongono che il titolare del trattamento stabilisca adeguate misure di sicurezza per il trattamento dei dati, sia da un punto di vista informatico, che giuridico. Questi principi integrano e rinnovano l'impianto di tutele che era stato già predisposto all'interno della Direttiva 95/46/CE.

In seguito, all'interno dell'articolo 6 GDPR troviamo espresse le condizioni di liceità del trattamento. Affinché il trattamento di dati biometrici risulti lecito, esso deve fondarsi su una base giuridica legittima e sul consenso dell'interessato. In particolare, il trattamento può essere ritenuto lecito solo nella misura in cui ricorra almeno una delle seguenti condizioni (art. 6, par.1 GDPR):

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore[53].

Il secondo paragrafo dell'art. 6 GDPR stabilisce invece che gli Stati membri possano mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del regolamento con riguardo al trattamento, in conformità del par.1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito.

[53] La lettera f) del primo paragrafo non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Sulla base delle innovazioni introdotte dal GDPR[54] il trattamento dei dati biometrici dovrà essere conforme anche ai principi della *data protection by design* (art. 25, par. 1) e *data protection by default* (art. 25, par. 2). Con la prima espressione si intende il principio in base al quale il titolare del trattamento ha l'obbligo di adottare misure tecniche e organizzative che garantiscano la maggiore riservatezza possibile al dato, oppure che trattino i dati in modo da minimizzarne l'uso[55].

In sostanza la data protection by design implica che già dalle prime fasi del trattamento esso sia strutturato per riflettere nel modo più efficace le prescrizioni del GDPR. Tuttavia, i principi del GDPR non devono essere solo garantiti *ex ante* nell'impostazione del trattamento, ma essere implementati in ogni sua fase, specialmente nell'ambito della sua esecuzione. Ed è qua che il primo concetto viene integrato dal suo complementare: la data protection by default.

Il secondo principio prevede lo sviluppo di tecniche idonee a implementare i principi della disciplina sulla protezione dei dati all'interno delle fasi del trattamento. Si tratta di un concetto essenziale nel caso dei dati biometrici, in quanto ad essi in genere si applicano forme di trattamento automatizzato. Sulla base di questo principio si stabilisce come in questi casi la protezione dei dati personali debba essere garantita da impostazioni predefinite (per l'appunto di "default")[44]. Da un punto di vista operativo, nel caso dei dati biometrici, questo implica che sia fortemente incoraggiato l'utilizzo di *privacy-enhancing technologies (PETs)*[56].

Le PETs possono essere introdotte sia da parte di soggetti pubblici, che privati e consistono in tecnologie o prodotti software finalizzati alla protezione e al rafforzamento della protezione della privacy[57]. Costituiscono esempi di PETs i dispositivi per bloccare i cookies, software in grado di garantire l'anonimato, sistemi di cifratura e lo *standard P3P (Platform for Privacy Preferences)*[58]. Inoltre, l'inquadramento del dato biometrico all'interno della disciplina del dato sensibile (art. 9, par. 1), comporta l'applicazione di alcune disposizioni ulteriori tratte da materie specifiche[59]. Parte della dottrina ha evidenziato come in materia di informazione da fornire all'interessato, qualora il trattamento sia fondato sul consenso dell'interessato, il titolare del trattamento dovrà esplicitarne il diritto di revoca del consenso esercitabile in qualsiasi momento (art. 13, par. 2, lett. c) e art. 14, par. 2, lett. d) GDPR). Un altro caso concerne la disciplina del diritto all'oblio[60], secondo la quale il titolare

[54] M. Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information,* cit. p. 382-389.
[55] M. Soffientini, *Privacy, protezione e trattamento dei dati*, cit., p. 97-98.
[56] R. Ducato, *I dati biometrici*, cit., p. 1315.
[57] Garante per la protezione dei dati, "*Tecnologie a protezione dei dati. Indagine conoscitiva della Commissione".* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1680228
[58] Si tratta di un protocollo che consente di confrontare le proprie impostazioni sulla privacy con quelle dei siti web che hanno aderito al protocollo, per poter acquisire conoscenza dei possibili rischi e valutare autonomamente se procedere nella navigazione.
[59] C. Jasserand, *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, cit., p. 307-311.
[60] C.d. "diritto all'oblio", secondo la definizione del Garante per la privacy si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. https://www.garanteprivacy.it/regolamentoue/oblio

del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali se l'interessato revoca il suo consenso e non esiste un ulteriore fondamento giuridico per il trattamento (art. 17, par. 1, lett. b) GDPR). Secondo l'art. 17, par.1 lett. a) se il trattamento è basato sul consenso, l'interessato ha diritto alla portabilità del dato. In aggiunta, un soggetto non può essere soggetto a forme di trattamento automatizzato a meno che vi sia il consenso dell'interessato o il trattamento sia giustificato da motivi di interesse pubblico rilevanti sulla base del diritto dell'Unione o degli Stati membri, in modo proporzionato alla finalità perseguita, ai sensi dell'art. 9, par. 2 lett a) e lett. g). Da ultimo, se il trattamento coinvolge la raccolta di dati sensibili, gli obblighi relativi alle attività di trattamento devono applicarsi anche alle imprese con un numero di dipendenti inferiori ai 250 (art. 30, par. 5, GDPR).

Se il trattamento viene effettuato su larga scala, il titolare del trattamento deve effettuare il *data protection impact assessment*[61] ai sensi dell'art. 35 GDPR e procedere alla nomina del responsabile della protezione dei dati ai sensi dell'art. 37 GDPR. La valutazione di impatto sulla protezione dei dati non viene richiesta solo nei casi concernenti il trattamento di dati sensibili, ma anche in due ulteriori condizioni[62]. In particolare essa deve applicarsi se il titolare del trattamento effettua una valutazione sistematica e globale di aspetti relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche (art. 35, par. 3, lett. a); oppure nel caso di una sorveglianza su larga scala di una zona accessibile al pubblico (art. 35, par. 3, lett. c). Anche la nomina del responsabile della protezione dei dati può essere estesa ad ulteriori ipotesi rispetto a quelle legate al trattamento di dati sensibili[63].

Questa nomina infatti si rende necessaria anche nel caso in cui il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali (art. 37, par. 1, lett a) o se il trattamento riguardi un ambito di applicazione che per sua natura richiede un monitoraggio regolare e sistematico degli interessi su larga scala (art. 37, par. 1, lett. b)[51]. Dopo aver ricostruito le previsioni applicabili ai dati biometrici nel nuovo Regolamento europeo, resta un'ultima innovazione importante da contestualizzare per quanto concerne la supervisione di queste nuove misure: la nascita del Comitato europeo per la protezione dei dati (EDPB), l'organismo che ha sostituito il Gruppo di lavoro articolo 29 (previsto

[61] Valutazione di impatto sulla protezione dei dati (DPIA), è un onere posto a carico del titolare del trattamento, essa serve a valutare i fattori di rischio connessi al trattamento posto in essere, analizzando le conseguenze del trattamento ed il loro impatto sui diritti e le libertà degli interessati.

[62] R. Ducato, *I dati biometrici*, cit., p. 1318-1320.

[63] M. Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information,* cit., p. 389-392.

dall'art. 29 della direttiva 95/46/CE), con l'introduzione del GDPR ed ha una funzione di raccordo fra le varie autorità nazionali di vigilanza e protezione dei dati. L'EDPB è un organismo consultivo indipendente, composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta. Le decisioni sono adottate a maggioranza semplice dei rappresentanti delle autorità di controllo[64].

Questo nuovo organismo si affianca al già preesistente Garante europeo per la protezione dei dati (EDPS), istituto dal Regolamento CE 45/2001, al quale però di fatto non si applica la disciplina del GDPR. Prima della sua introduzione, l'EDPS era la sola autorità di diritto europeo nell'ambito della protezione dei dati, anche se la sua competenza era limitata dai trattati delle istituzioni dapprima della Comunità economica ed in seguito dell'Unione Europea. Dal 25 maggio 2018, invece, abbiamo la compresenza di due organi europei in materia di protezione dei dati personali, che differiscono nella composizione, nelle competenze e nelle basi giuridiche che ne legittimano l'istituzione. A tal fine è necessario sottolineare come l'EDPB sia l'unico organo europeo istituito e riconosciuto dal GDPR, il solo che riunisce tutte le Autorità nazionali indipendenti ed eserciti un controllo su di esse nell'applicazione delle previsioni del nuovo Regolamento e che possa decidere nel caso di eventuali controversie sulla loro competenza[65]. Pertanto ad oggi si deve attribuire un ruolo primario al Comitato europeo per la protezione dei dati. L'EDPS invece ha una diversa base istitutiva, competenze limitate ad aspetti organizzativi dell'Unione Europea e agli atti giuridici che rientrano nell'ambito di applicazione del Regolamento 45/2001 CE[66]. L'art 2, paragrafo 3 del GDPR sancisce che per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione si applichi il Regolamento n. 45/2001 CE. Il medesimo paragrafo ha imposto ai legislatori europei l'adeguamento del testo del Regolamento n. 45/2001 CE alle previsioni introdotte dal GDPR. Con l'approvazione del Regolamento UE n. 2018/1725[67] del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, sono stati abrogati il regolamento n. 45/2001 CE e la decisione n. 1247/2002/CE.

---

[64] Dal sito ufficiale dell'European Data Protection Board: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_it

[65] F. Pizzetti, *Il Nuovo Comitato europeo per la protezione dei dati (EDPB), dopo il GDPR: compiti e poteri*, in *Agenda Digitale*, 31 maggio 2018.
https://www.agendadigitale.eu/sicurezza/il-nuovo-comitato-europeo-per-la-protezione-dei-dati-edpr-dopo-il-gdpr-compiti-e-poteri/

[66] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in G.U.C.E. L 8/1.

[67] Regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE, in G.U.U.E. L 295/39.

2.2 Criticità e problemi: le categorie di dato biometrico

Attraverso l'introduzione del GDPR il dato biometrico ottiene finalmente una sua autonomia concettuale. Come ci mostra il dibattito in dottrina, però, la sua definizione non è esente da alcuni cavilli interpretativi. Secondo il testo del GDPR il dato biometrico rappresenta una forma particolare di dato personale, costituita da quell'informazione collegata alle caratteristiche fisiche e comportamentali di un soggetto, ottenuta tramite un procedimento tecnico e volta all'identificazione univoca o alla conferma dell'identità[68]. La definizione però non chiarisce alcuni aspetti tecnici, quali la natura del procedimento con cui i dati vengono raccolti. Inoltre, si individua nell'aspetto identificativo il fattore chiave per giustificare l'inserimento del dato biometrico all'interno dell'elenco dei dati sensibili all'art. 9 GDPR, ma la qualifica di dato sensibile viene riconosciuta espressamente solo ai dati biometrici "intesi a identificare in modo univoco una persona fisica" e non ai dati biometrici nel loro insieme. Pertanto la natura di dato sensibile sembra essere riconosciuta solo ad alcune categorie di dati biometrici, lasciandone altre escluse da questa forma di tutela più estesa. Questo ci pone però di fronte ad un primo elemento critico: se l'obiettivo primario del legislatore era quello di tutelare le libertà ed i diritti fondamentali che potrebbero risultare compromessi dal trattamento dei dati biometrici, un regime di protezione più alto dovrebbe essere giustificato a prescindere dalla finalità della loro raccolta, specialmente in virtù del loro legame irreversibile con l'identità di un soggetto specifico. Secondo parte della dottrina, ponendo questa distinzione artificiale fra le varie categorie di dati biometrici, il nuovo regolamento non riesce a fornire regole esaustivamente chiare e una protezione adeguata al rispetto dei diritti e delle libertà fondamentali. Inoltre alcuni elementi tecnici essenziali quali la raccolta, lo stoccaggio e la conservazione di questi dati non vengono affrontati in dettaglio, mentre gli Stati membri vengono lasciati soli nell'adozione di ulteriori norme nazionali più stringenti e specifiche, che ad oggi si rivelano quanto più urgenti per far fronte alla regolazione del mercato relativo a queste tecnologie. In cinque delle dieci esenzioni dell'articolo 9, par. 2, GDPR è necessaria una normativa supplementare dell'Unione europea o degli Stati membri che fornisca garanzie per i diritti e gli interessi fondamentali delle persone interessate. Questo complesso quadro giuridico nazionale e sovranazionale rischia di rivelarsi particolarmente oneroso per le aziende che utilizzano questi dati. L'obiettivo di tracciare un equilibro fra la libera circolazione dei dati biometrici e la protezione dei cittadini non sembra essere stato ancora raggiunto[69]. Uno dei fattori maggiormente critici riguarda le banche dati all'interno delle quali vengono archiviati i dati biometrici. All'interno di esse, la tecnologia biometrica consente di

[68] R. Ducato, *I dati biometrici*, cit., p. 1321.
[69] E. J. Kindt, *Having yes, using no? Abaout the new legal regime for biometric data*, in *Computer Law & Security Review 34*, 2018, p. 523-525.

effettuare un confronto tra le informazioni biometriche acquisite in tempo reale o raccolte in altro modo e i dati registrati all'interno delle banche dati preesistenti. In questo modo risulta immediato e automatico identificare direttamente una persona, basandosi su caratteristiche fisiche, fisiologiche o comportamentali. Il numero di queste banche dati biometriche sta crescendo a ritmi estremamente elevati, sia nelle mani di enti pubblici che privati. Di fatto, l'archiviazione centrale dei dati biometrici, consentendo una rapida identificazione degli individui, cambia la configurazione degli spazi pubblici e privati e influisce sempre maggiormente anche nella definizione delle attività di governo, polizia e intelligence. La tecnologia biometrica può senz'altro rivelarsi estremamente utile per scopi specifici quali la ricerca scientifica o il contrasto al crimine da parte delle autorità competenti, ciò sempre all'interno di chiare condizioni legali e di una supervisione indipendente, ma qualsiasi uso diffuso di queste tecnologie senza un chiaro quadro legale dovrebbe destare preoccupazione.

Mentre gli individui esercitano più o meno normalmente un controllo sull'identificazione non automatizzata, fornendo informazioni identificative ad altri in modo consapevole, ciò non avviene con la tecnologia biometrica, che avvalendosi di sistemi automatizzati rende molto più semplice e immediato l'appropriarsi di informazioni specifiche su di particolari individui, anche senza che essi ne siano pienamente consapevoli. Se in dottrina non vi è conflitto sul divieto generale di trattamento dei dati biometrici a scopo di identificazione[70] sancito dall'art. 9, par. 1, GDPR e sull'introduzione di forme obbligatorie di DPIA, viene fortemente dibattuta invece la scelta di concentrarsi solo su di un loro uso specifico senza interrogarsi sulla natura stessa di questi dati e regolare puntualmente la creazione e l'uso di banche dati biometriche. La protezione legale e la valutazione di impatto sul trattamento di dati biometrici dovrebbero focalizzarsi proprio sulle modalità di raccolta e di archiviazione di questi dati contenenti caratteristiche uniche, atte all'identificazione e alla verifica di una persona. Attualmente sulla base delle prescrizioni del GDPR è possibile distinguere almeno quattro diverse categorie di dati biometrici sottoposte a forme più o meno stringenti di regolazione[71].

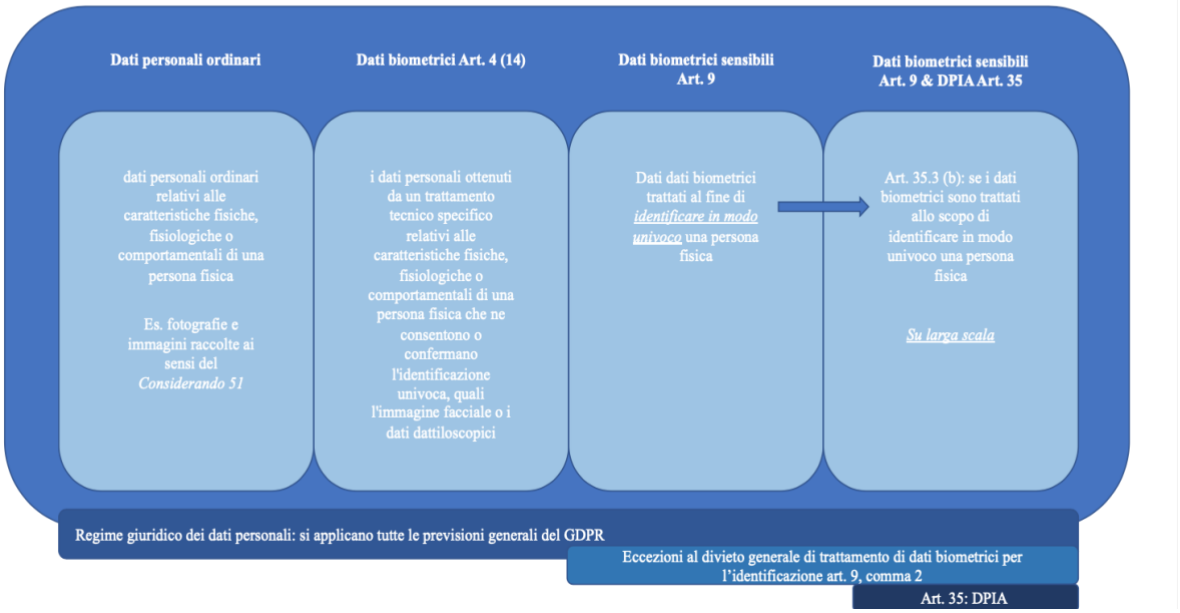
In primo luogo, abbiamo i dati personali ordinari relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica. Essi sono ritenuti semplici e ordinari, in quanto non possono essere ritenuti dati biometrici finché non vengono trattati attraverso un mezzo tecnico specifico che consenta l'identificazione o l'autenticazione unica di una persona fisica. Quindi la raccolta di questa tipologia di dati, anche se si riferiscono a caratteristiche umane uniche e insostituibili, non è soggetta ad alcun regime biometrico o di protezione specifico e rientra nella legislazione generale sulla privacy e sulla protezione dei dati del GDPR. Ne fanno parte ad esempio le fotografie di bambini in un archivio scolastico o i database di agenzie governative, che non costituiscono dati biometrici se non

[70] J. Andrew, M. Baker, *The General Data Protection Regulation in the Age of Surveillance Capitalism*, in *Journal of Business Ethics*, 2021, 168, p. 570-573.
[71] E. J. Kindt, *Having yes, using no? Abaout the new legal regime for biometric data*, cit., p. 534-535.

sono trattati da un sistema biometrico[72].In secondo luogo, troviamo i dati biometrici ai sensi della definizione dell'art. 4, par. 14 GDPR, ossia i dati personali risultanti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che consenta o confermi la sua identificazione unica. Di fatto, non esiste un regime giuridico specifico attribuibile a questa categoria (esclusi i dati biometrici utilizzati per l'identificazione univoca) se non gli obblighi generali sanciti dal GDPR per i dati personali. Questa categoria e la prima sono soggette pertanto al medesimo regime giuridico dei dati personali ordinari. La terza categoria riguarda i dati biometrici trattati per identificare in modo univoco una persona fisica, ai sensi dell'art. 9, par. 1, GDPR. A questa tipologia di dati biometrici viene esteso il regime giuridico specifico per la protezione dei dati sensibili. L'uso di questi dati in sistemi di identificazione risulta in linea di principio vietato, escluse le eccezioni elencate all'interno del secondo paragrafo del medesimo articolo. Infine, nell'ultima categoria abbiamo i dati biometrici trattati ai fini dell'identificazione univoca su larga scala, che deve essere conforme oltre agli obblighi generali di protezione dei dati, alle previsioni dell'art. 9 GDPR e dell'art. 35 GDPR che prevede l'introduzione della valutazione di impatto sulla protezione dei dati.

Queste categorie possono essere esemplificate concettualmente attraverso una rappresentazione grafica:

Tabella 1 – Le categorie di dati biometrici all'interno del GDPR



Fonte: E. J. Kindt

[72] La raccolta e la memorizzazione di immagini facciali non rientrano in nessun regime di protezione dei dati biometrici specifico e rafforzato.

Da ultimo possiamo affermare come il nuovo quadro giuridico introdotto dal GDPR consenta la raccolta dei dati biometrici sulla base di disposizioni di applicazione generale e attraverso l'impiego di banche dati, regolando però solo l'uso specifico di tali dati. Sulla base della definizione di dati biometrici e di ulteriori distinzioni interne al GDPR è possibile individuare quattro diverse categorie di dati personali relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne permettano la verifica dell'identità o l'identificazione. A queste categorie si applicano regimi giuridici diversi, inoltre secondo il GDPR l'uso di dati biometrici per l'identificazione è in linea di principio vietato, salvo alcune eccezioni. Ai responsabili è attribuito anche il compito di effettuare nei casi richiesti la valutazione di impatto della tecnologia biometrica ai sensi dell'art. 35 GDPR ed in alcuni casi persino richiedere un'autorizzazione preventiva.
Il divieto generale di trattamento di dati biometrici per l'identificazione costituisce una misura essenziale per bilanciare i gravi rischi per le libertà ed i diritti fondamentali in cui incorreremmo senza di esso. Tuttavia resta controverso l'approccio del legislatore europeo, volto ad approfondire solo l'uso dei dati biometrici, tralasciando fattori essenziali quali la loro raccolta e conservazione in appositi *database*, dato che è proprio a partire dalla raccolta dei dati e dalla loro conservazione che si ottiene il primo tassello per effettuare l'identificazione degli individui. Come già analizzato inizialmente a questo proposito la disciplina europea antecedente al GDPR ha più volte sottolineato i rischi connessi alla conservazione di questa tipologia di dati in banche dati centralizzate, ma resta ancora da definire un regime giuridico specifico per i dati biometrici *tout court*.

3. I diritti fondamentali minacciati dall'impiego dei dati biometrici

I sistemi biometrici hanno campi di sviluppo e applicazione molto ampi e variegati. Da un lato, le loro enormi potenzialità hanno attirato gli investimenti di soggetti privati e grandi aziende, che hanno impiegato i dati biometrici per garantire l'accesso a servizi, l'attivazione di dispositivi elettronici, sfruttare sistemi di Intelligenza Artificiale e di Machine Learning, oppure all'interno del settore bancario, per identificare dei soggetti titolari dei conti bancari o di altri servizi[73]. Inoltre, in alcuni paesi si è ipotizzato un uso della biometria per contrastare la lotta all'assenteismo e controllare gli accessi dei dipendenti sui luoghi di lavoro. Anche all'interno del settore pubblico, però, queste tecnologie stanno assumendo un ruolo sempre più rilevante. Attualmente il riconoscimento biometrico viene impiegato in misure tese a migliorare la sicurezza pubblica o nazionale[74], per agevolare lo sviluppo di indagini penali, contrastare la criminalità organizzata e garantire il controllo

[73] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy* Regulation, cit., p. 229-231.
[74] R. Das, *The science of Biometrics: Security technology for identity Verification*, Routledge, 2019, p.70-76.

delle frontiere e finalità antiterroristiche, oltre ad implementare l'efficienza di numerosi servizi pubblici[75]. L'incessante sviluppo e commercializzazione di questi sistemi di determinazione biometrica all'interno di più settori può rivelarsi però estremamente insidiosa e comportare numerosi rischi connessi allo sfruttamento di questi sistemi, specialmente per quanto concerne il rispetto dei diritti e delle libertà fondamentali dei suoi utenti[76].I dati biometrici sono caratterizzati dalla loro unicità e insostituibilità, che rende impossibile mutarli o sostituirli con altre informazioni se sottratti e utilizzati indebitamente, senza il consenso degli interessati. Con l'introduzione del GDPR la notificazione preventiva di queste violazioni è stata abolita e sostituita da nuovi obblighi di tenuta di un registro dei trattamenti e dell'introduzione della "*data breach notification"*.

Il dovere di notificazione delle violazioni dei dati personali prevede che i titolari di trattamento debbano notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e senza ingiustificato ritardo, a meno che risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 33, par. 1 GDPR. Come si evince la *data breach notification* non è obbligatoria, ma dipende dalla valutazione dei rischi effettuata dal titolare del trattamento[77].

Ad ogni titolare viene però attribuito l'obbligo di documentare le violazioni di dati riscontrate, anche se non comunicate all'Autorità di controllo e gli interessati, nonché le relative circostanze, conseguenze e i provvedimenti adottati all'interno di un apposito registro (art. 33, par. 5 GDPR).

Ai sensi dell'art. 34 GDPR quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo[78].

Oltre al rischio di diffusione illecita dei dati, vi è anche il pericolo legato all'incrocio indebito di dati biometrici con altre informazioni personali noto come *function creep*[79], difficilissimo da scoprire e impedire da parte dell'interessato, che può comportare vere e proprie attività nascoste di profilazione di soggetti[80]. Il *Considerando 91* specifica i rischi connessi all'uso di sistemi di profilazione basati su dati biometrici. Inoltre, si deve anche considerare che da questi dati è possibile trarre un ampio novero di informazioni sensibili. Ad esempio, la struttura vascolare di una mano può rilevare la presenza di alcune malattie cromosomiche oppure la rilevazione della firma può determinare la

[75] G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, cit., p. 1109.
[76] T. B. Gillis, J. L. Spiess, *Big Data and Discrimination*, cit., 464-465.
[77] M. Soffientini, *Privacy, protezione e trattamento dei dati*, cit., p. 167 – 168.
[78] Ai sensi dell'Art. 34, par. 3 GDPR non è richiesta la comunicazione all'interessato di cui al par. 1 se è soddisfatta una delle condizioni descritte dalle lett. a) b) e c).
[79] Per *function creep* si intende il graduale ampliamento dell'uso di una tecnologia o di un sistema oltre lo scopo per il quale è stato originariamente previsto, specialmente quando ciò comporta una potenziale violazione della privacy (definizione dizionario inglese Collins).
[80] L'attività di profilazione è definita all'art. 4, par. 4 GDPR.

presenza di malattie neurologiche[81]. Nell'analizzare i rischi connessi all'uso di sistemi di riconoscimento biometrico, si deve inizialmente porre una distinzione tecnica fra i due principali modelli che contraddistinguono questi sistemi, di cui il primo mette in atto una mera "verifica", mentre il secondo identifica puntualmente l'identità del soggetto[66]:

- Approccio *one-to-one*: confronta il dato rilevato con i dati raccolti precedentemente ed inseriti all'interno di un unico supporto, ad esempio durante l'emissione di un documento o di un badge di lavoro; rientrano in questo modello il caso delle carte d'identità elettroniche e i lettori di impronte digitali nei propri smartphone

- Approccio *one-to-many*: confronta il dato biometrico raccolto con i dati di un numero elevato di soggetti precedentemente rilevati e conservati all'interno di una banca dati, controllando la corrispondenza del dato con ognuno di essi;
  avviene attraverso una prima fase di acquisizione del dato dall'utente con la sua conservazione su supporto unico e una seconda fase di autenticazione, basata sull'attività di *matching*, effettuata confrontando il dato corrente con i dati memorizzati a livello centralizzato tramite appositi algoritmi;

In base a questa definizione si definisce anche l'entità dei rischi connessi alla tutela della riservatezza degli utenti e l'estensione delle misure messe in atto. Il secondo modello comporta una maggiore pericolosità per la tutela dei diritti alla riservatezza e alla protezione dei dati, in quanto la conservazione dei dati su larga scala all'interno di un unico *database*, li rende maggiormente esposti a rischi di sottrazione indebita. Inoltre, nei sistemi one-to-many risultano statisticamente maggiori gli errori algoritmici nelle procedure di identificazione, come ad esempio i falsi match. Nonostante ciò queste procedure vengono adottate estensivamente per la loro capacità di garantire un maggiore controllo, rendendo più semplice sventare frodi o scambi di persone[82]. Il quadro tracciato fin qui serve a delineare come i sistemi di identificazione biometrica possano incidere fortemente su una molteplicità di diritti fondamentali. I primi diritti ad essere coinvolti nell'uso di queste tecnologie sono senz'altro i diritti connessi alla tutela della privacy[83]. Essa viene generalmente intesa nella sua accezione negativa, come diritto alla conservazione della propria sfera privata, lontana da ingerenze

[81] G. Formici, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, cit., p. 1110-1111.
[82] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* in *Boston College Law Review*, 2019, p. 354-357.
[83] G. Mobilio, *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale,* in *Consulta Online*, 2021 Fasc. III, p. 743-746.

altrui. Questo diritto è direttamente connesso al diritto alla riservatezza, il quale afferma come nessun individuo possa essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né ad alcuna lesione del suo onore e della sua reputazione[84]. I sistemi biometrici interferiscono notevolmente con questi diritti, in quanto l'uso di queste tecnologie conferisce estesi poteri di controllo e tracciamento alle aziende ed enti che ne facciano utilizzo. Gli attuali strumenti di analisi dei big data consentono inferenze predittive estremamente accurate, nonché una maggior abilità nell'influenzare le scelte dei consumatori, studiare i loro comportamenti, mettendo notevolmente a rischio l'integrità delle loro sfere private.

Altri diritti fortemente influenzati dall'adozione di questi sistemi sono quelli legati alla protezione dei dati personali, definita come il diritto di ogni individuo alla protezione dei dati di carattere personale che lo riguardano[85]. Essa è da intendersi come la giusta pretesa di ogni individuo a poter esercitare un controllo accurato sull'insieme di dati che costituiscono la proiezione della sua persona nella società dell'informazione[69]. La tutela di questo diritto diventa centrale in un contesto come quello attuale caratterizzato dalla progressiva codificazione della nostra società, attraverso processi di conversione di flussi di dati elaborati da algoritmi in informazioni spendibili per obiettivi molto variabili. Se i sistemi biometrici consentono ad attori pubblici e privati di rilevare sistematicamente i nostri dati personali per studiare e monitorare le nostre attività, i diritti per la protezione dei nostri dati diventano essenziali nel porre delle limitazioni a queste forme di controllo, tutelando l'universo delle nostre relazioni online ed offline. Anche il diritto all'integrità della propria identità personale risulta coinvolto nell'uso di queste tecnologie.

Il rispetto della propria identità digitale, intesa come la proiezione di sé e della propria immagine nel contesto virtuale, resta un elemento primario a fronte dei constanti processi di datificazione sopra menzionati[72]. L'interferenza con questa tipologia di diritti avviene in relazione alle informazioni estraibili dal trattamento dei dati biometrici del soggetto in questione: in particolare informazioni relative ad altri dati sensibili quali il genere, l'appartenenza etnica, le opinioni politiche o l'orientamento sessuale. Queste informazioni una volta estratte possono contribuire a classificare un soggetto all'interno di gruppi definiti come *cluster*. Tramite questi gruppi, costituiti in base a simili elementi informativi che ne determinano l'appartenenza, l'identità del soggetto risulta frammentata e processata per riflettere un profilo standard di analisi in base al quale si procede alla profilazione delle sue attività online. L'identità del singolo soggetto viene pertanto così ricondotta a uno schema predefinito, che prescinde la sua individualità. Da ultimo, i sistemi biometrici possono dar luogo a numerosi fenomeni discriminatori, determinati dalle distorsioni presenti all'interno dei sistemi

[84] Art. 12 della Dichiarazione Universale dei Diritti dell'Uomo.
[85] Art. 8 Carta dei diritti dell'Unione Europea.

informatici e algoritmici[72]. Gli algoritmi impiegati in processi di identificazione biometrica si basano su campioni di dati che spesso riflettono in modo distorto la rappresentazione della popolazione o che possono rivelare pregiudizi impliciti. Un esempio emblematico della portata di questi fenomeni è dato dalla commercializzazione di software per il riconoscimento facciale. Quando si tratta della rilevazione dei tratti dei nostri volti diventa difficile esercitare il nostro diritto all'oblio ed eliminare la nostra presenza online. I dati biometrici dei nostri volti non possono essere disinstallati così semplicemente come il profilo attivo su un social network o la nostra email. La commercializzazione di sistemi di sorveglianza di questo tipo può avere un enorme impatto sulle vite delle persone, condizionando le loro scelte quotidiane. Per esempio, un individuo potrebbe avere timore nel prendere parte a un evento pubblico come una manifestazione o un corteo per paura di essere ripreso, limitando un suo diritto essenziale quale la libertà d'espressione, principio cardine su cui si fondano le nostre democrazie[86]. Se l'obiettivo principale diventa la rilevazione dei nostri volti com'è possibile tutelarsi e poter garantire il proprio anonimato?

Secondo le Linee guida sul riconoscimento facciale, adottate dal Comitato consultivo della Convenzione 108 nel gennaio 2021[87], la base per regolare questo potere di controllo deve essere fondata sulla conoscenza e sul consenso al trattamento da parte degli interessati. I soggetti coinvolti devono avere la possibilità di esprimere un libero consenso al trattamento dei loro dati biometrici, inoltre l'adozione di un simile sistema di sorveglianza deve essere giustificato da principi di necessità e proporzionalità. Per tanto non è concesso un uso di questi sistemi che vada a limitare altre libertà fondamentali, quali la libertà di espressione o di associazione. L'obiettivo per il legislatore europeo dovrebbe essere quello di garantire un giusto bilanciamento fra l'utilità di questi sistemi e la loro ingerenza nei diritti e libertà fondamentali delle persone.

Un altro aspetto che desta non poca preoccupazione in riferimento ai sistemi di riconoscimento facciale, riguarda l'elevata componente di errori statistici che li caratterizza e la loro tendenza a determinare fenomeni discriminatori. Questi algoritmi finalizzati al riconoscimento biometrico causano spesso numerosi errori nella lettura dei volti, specialmente nei casi che coinvolgono donne, bambini, persone di colore e persone affette da disabilità[88]. Pertanto la crescente commercializzazione di questi sistemi pone un notevole incremento nelle violazioni del principio di non discriminazione[89]. Recentemente ha destato stupore come il software di riconoscimento facciale, ideato da Amazon

[86] F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 2021, p. 213-215.
[87] Consultative Committee of the convention for the protection of individuals with regard to automatic processing of personal data, Convention 108, *Giudelines on Facial Recognition*, 28 gennaio 2021, T-PD (2020)03rev4.
[88] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* cit., p. 350-354.
[89] T. B. Gillis, J. L. Spiess, *Big Data and Discrimination*, cit., p. 460-466.

(commercializzato pure in Europa) e testato sui membri del Congresso americano, abbia erroneamente identificato 28 di essi di etnia afroamericana come potenziali criminali, ricollegando le loro immagini ad alcune foto segnaletiche presenti nel suo database[90]. Episodi di questo tipo testimoniamo la fallibilità di queste tecnologie e dovrebbero farci riflettere sull'effettiva esigenza di una loro applicazione massiva a fronte di rischi così elevati per i diritti alla privacy, alla libertà di espressione e per la garanzia del principio di non discriminazione.

4. Il trattamento di dati biometrici

Come già osservato, il GDPR fornisce una disciplina generale ai dati biometrici, definendo le condizioni di ammissibilità del loro trattamento all'interno degli artt. 6 e 9. Tuttavia, l'attività del legislatore europeo dovrebbe essere coadiuvata dalle sinergie dei legislatori dei singoli Stati membri per integrarne la disciplina all'interno del loro diritto nazionale (specialmente per quanto concerne i profili della loro raccolta e conservazione in banche dati). Attualmente però, all'interno del contesto europeo nessuno Stato ha ancora elaborato e introdotto una disciplina giuridica di rango primario rivolta ai sistemi biometrici[91].

La carenza di una normativa nazionale puntuale sulla biometria che integri il modello europeo, riflette le difficoltà che questi sistemi pongono ai nostri legislatori. Ciò è attribuibile in primo luogo alla velocità con cui si producono e diffondono queste innovazioni tecnologiche, mentre il procedimento legislativo richiede delle procedure ed elaborazioni molto più lente e dilatate nel tempo. Inoltre, la ricerca nello sviluppo di questo settore viene condotta essenzialmente da attori privati, colossi del digitale, che detengono il capitale economico necessario alla commercializzazione di questi sistemi nel mercato globale. Queste multinazionali ad oggi detengono un patrimonio conoscitivo di questi sistemi che risulta irraggiungibile per i pubblici poteri[92]. Questi ultimi hanno avuto solo un approccio tardivo alla biometria, riconoscendo i rischi di questi sistemi solo quando la loro diffusione era già largamente avviata e difficile da limitare. A fronte di una domanda di mercato in forte crescita e del vuoto normativo prodotto dall'indecisione legislativa, sono questi attori economici a dover generalmente assumere un ruolo decisionale, elaborando autonomamente delle limitazioni[93]. Questi attori privati, assumendo un ruolo semi-pubblicistico, agiscono ormai come intermediari necessari

[90] M. DeGeurin, *Amazon's Facial Recognition Software Mistakes 28 Cogressmen for Criminals*, in *Intelligencer*, *The New York Magazine*, 27 luglio 2018. https://nymag.com/intelligencer/2018/07/amazon-rekognition-mistakes-congressmen-for-criminals-aclu.html

[91] G. Mobilio, *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale*, cit., p. 740.

[92] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* cit., p. 350-354.

[93] R. Das, *The science of Biometrics: Security technology for identity Verification*, cit., p.70-76.

per la predisposizione di misure adeguate alla tutela dei diritti fondamentali minacciati dall'uso di questi sistemi[94]. Alcune multinazionali, quali IBM[95] ad esempio, hanno deciso di sospendere il commercio di alcuni sistemi di identificazione biometrica per le troppe interferenze con il diritto alla privacy e le forme di discriminazione determinate dalle imperfezioni algoritmiche alla base del loro funzionamento[96]. Pertanto, abbiamo un contesto ibrido all'interno del quale, a fronte delle limitazioni poste dal GDPR, sono questi soggetti privati a determinare come e a quali condizioni consentire il commercio di queste tecnologie. Inoltre anche il settore pubblico, ricorrendo sempre maggiormente alla biometria in ambiti di pubblica sicurezza e contrasto al terrorismo, deve necessariamente affidarsi ad operatori privati per acquisire questi sistemi. Il recente avvento della pandemia globale da Covid-19 ha determinato l'uso crescente di sistemi di biometrici da parte di soggetti pubblici per misurare la temperatura corporea, rilevare i volti senza mascherina in spazi pubblici e tracciare i contagi, testimoniando come i governi e le aziende si stanno rivolgendo a nuovi usi delle tecnologie biometriche per limitare il contagio e svilupparne le opportunità economiche[97].

Gli operatori economici che detengono il commercio di questi sistemi in termini monopolistici risultano in possesso anche di una risorsa conoscitiva senza precedenti, frutto dell'elaborazione di tecnologie in grado di raccogliere massivamente dati, che se combinati con i sistemi di *data analysis* possono determinare informazioni estremamente accurate sulle abitudini, gli spostamenti e l'identità degli utenti interessati[98]. Non a caso la docente di Harvard Shoshana Zuboff, analizzando la genesi di questi sistemi, ha definito i dati biometrici la nuova valuta dell'economia digitale[99], arrivando a teorizzare l'emersione di un vero e proprio "capitalismo della sorveglianza", dimostrando come i modelli di business adottati dai colossi del digitale (quali Facebook, Amazon e Google) generino nuove forme di accumulazione capitalista. È necessario evidenziare come il ruolo monopolistico ricoperto da queste multinazionali nel mercato digitale assuma anche un valore politico di primo piano, in quanto sono questi soggetti a determinare le condizioni per il commercio di questi sistemi e a detenere un forte potere nei confronti delle autorità pubbliche. Attualmente, le aziende private possono infatti scegliere se concedere a istituzioni e soggetti pubblici l'acquisto di questi sistemi e quali informazioni condividere con essi. Quindi oltre ad avere un peso economico decisivo, i colossi

[94] F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, cit., p. 216.
[95] A. Hern, *IBM quits facial-recognition market over police racial-profiling concerns*, 9 giugno 2020, The Guardian. https://www.theguardian.com/technology/2020/jun/09/ibm-quits-facial-recognition-market-over-law-enforcement-concerns
[96] T. B. Gillis, J. L. Spiess, *Big Data and Discrimination*, cit.p. 463-465.
[97] M. Van Natta, P. Chen, S. Herbek, et al., *The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic*, in *J Law Biosci*, 2020.
[98] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, cit., p. 233-235.
[99] S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019.

del digitale possono condizionare ampiamente i pubblici poteri, limitando il loro accesso a queste tecnologie, orientando la loro regolazione, intervenendo sulle forme di garanzia per diritti fondamentali e la tutela di libertà essenziali quali la libertà di espressione. Un altro elemento decisivo che emerge da queste considerazioni riguarda l'impossibilità di ricondurre l'uso dei sistemi biometrici alla giurisdizione di un solo ordinamento, data dalla commistione di una regolazione nazionale e sovranazionale. Inoltre, l'elaborazione di queste tecnologie algoritmiche proviene da contesti geograficamente estremamente diversi, che rendono ancora più complessa la determinazione della giurisdizione incaricata ad assolvere alle controversie in materia. Anche nel caso di forme di trattamento illecito di dati biometrici risulta difficile determinare l'organo titolare della giurisdizione in merito al caso. Tutti questi elementi concorrono a livello europeo anche nel rallentare l'aggiornamento della disciplina sulla responsabilità civile derivante dalle inefficienze di queste tecnologie, per individuare il soggetto responsabile al quale imputare i possibili danni[100]. A fronte del quadro fin qui delineato, di seguito provvederemmo ad analizzare in dettaglio le principali forme di trattamento applicabili ai dati biometrici sulla base del diritto europeo.

4.1 Il trattamento di dati biometrici in ambito commerciale

All'interno del contesto europeo, è il GDPR a determinare l'ambito di ammissibilità del ricorso a sistemi biometrici per scopi commerciali. Tale categoria di dati, come già visto, appartiene alla categoria di dati particolari di cui all'art. 9, par. 1 del GDPR, il cui trattamento risulta in linea generale vietato. Tuttavia vi sono delle situazioni di deroga elencate all'interno del secondo paragrafo del medesimo articolo che ne rendono ammissibile il trattamento. Nel caso del trattamento di dati biometrici all'interno del settore commerciale, l'esimente descritto alla lettera a) dell'art. 9, par. 2 GDPR costituisce la base giuridica su cui poter fondare questa tipologia di trattamento nei casi in cui:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

Pertanto il consenso preventivo costituisce l'unica base giuridica in grado di autorizzare il trattamento di dati biometrici all'interno dell'ambito commerciale. All'interno della disciplina del GDPR il consenso dell'interessato viene definito come "qualsiasi manifestazione di volontà libera, specifica,

[100] G. Mobilio, *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale,* cit., p. 741.

informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento" (art. 4, par. 1, n. 11 GDPR). Esso costituisce inoltre una delle condizioni di leicità del trattamento definite all'interno dell'art. 6, par. 1 GDPR, ai sensi del quale si stabilisce che il consenso debba essere libero, specifico, informato e inequivocabile. Non sono ammissibili forme di consenso tacite o presunte, il consenso deve essere prestato attraverso una dichiarazione positiva inequivocabile.Per far sì che il consenso prestato dal soggetto risulti informato è necessario dotare il soggetto dell'informativa sul trattamento. Sia il consenso che l'informativa costituiscono due presupposti di legittimità di un trattamento di dati personali. Secondo il *considerando 60* i principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. L'interessato deve essere pertanto informato su ogni aspetto relativo al trattamento dei propri dati, inclusa l'esistenza di attività di profilazione e le finalità della raccolta. L'informativa prestata al soggetto deve inoltre risultare coincisa, trasparente, facilmente accessibile, semplice idonea, in forma scritta e preferibilmente in formato elettronico[101].

Ai sensi dell'art. 7, par. 4 GDPR (condizioni per il consenso) nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Di fatto, affinché il consenso possa definirsi realmente libero nel caso di un trattamento di dati biometrici per fini commerciali, le aziende interessate devono garantire la possibilità di utilizzare un'alternativa tradizionale, ossia una forma di identificazione che non richieda l'impiego dei propri dati biometrici. Ad esempio, nel caso di sistemi di pagamento online che impieghino forme di autenticazione attraverso dati biometrici, l'utente deve avere la possibilità di utilizzare anche forme di autenticazione tradizionali, come l'uso di credenziali e password. Pertanto, il consenso dell'interessato si ritiene realmente privo di condizionamenti se risulta sempre presente sul mercato un'alternativa che consenta l'accesso al medesimo servizio senza l'obbligo di impiegare i propri dati biometrici. Secondo le linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, elaborate dall'European Data Protection Board[102], sul mercato di questi servizi o prodotti, risulta però alquanto difficile garantire una piena fungibilità fra sistemi che impiegano tecnologie biometriche e sistemi di autenticazione che non impiegano tecnologie biometriche. Questi sistemi posso differire sia per le specificità del prodotto/servizio al quale si riferiscono, sia per fattori geografici o per i processi di imitazione da parte di aziende competitrici, limitando la possibilità per uno stesso

[101] M. Soffientini, *Privacy, protezione e trattamento dei dati*, cit., p. 153-157.
[102] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 may 2020.

distributore di garantire in ogni evenienza la fungibilità di mercato. Inoltre, sempre secondo l'EDPB, nel caso specifico in cui la possibilità di scelta del soggetto risulti possibile solo fra il servizio di un distributore (che prevede il consenso al trattamento per finalità supplementari) e un servizio equivalente, che non richieda il trattamento di dati personali ma sia offerto da un altro distributore, il consenso dell'interessato non può considerarsi prestato liberamente in quanto in tal caso la scelta del soggetto dipenderebbe dall'offerta degli operatori concorrenti e non solo dalla valutazione della fungibilità per l'interessato[103].

4.2 I sistemi di autenticazione basati sul riconoscimento biometrico in ambito lavorativo

Al giorno d'oggi numerose aziende, sia nel settore pubblico che privato, decidono di adottare all'interno dei propri spazi sistemi di autenticazione basati sul riconoscimento biometrico per finalità organizzative o di sicurezza. Di conseguenza l'adozione di questi sistemi in ambito lavorativo richiede una valida base giuridica per questa tipologia di trattamento ai sensi dell'art 6 e dell'art. 9, par. 2 GDPR. Altra condizione di legittimità riguarda anche in questo caso la possibilità che il consenso prestato da parte dell'interessato possa ritenersi effettivamente libero ai sensi dell'art. 7, par. 4 GDPR. Come deliberato dal WP29 all'interno del parere 2/2017 sul trattamento dei dati sul posto di lavoro[104] in un contesto particolare come quello di un rapporto di lavoro dove esiste una relazione di subordinazione fra il datore di lavoro e i suoi impiegati, risulta difficile ipotizzare che il consenso al trattamento dei dati biometrici espresso dall'interessato sia espresso liberamente. Il soggetto impiegato potrebbe infatti temere delle rappresaglie da parte del suo superiore nel caso in cui rifiutasse di fornire il suo consenso.

Per far fronte a questo effettivo squilibrio di potere, fra l'interessato al trattamento ed il suo titolare, è necessario anche in questo caso garantire all'interessato la possibilità di impiegare una forma di autenticazione alternativa che non richieda l'utilizzo dei propri dati biometrici. Solo a questa condizione il consenso prestato dal soggetto interessato può ritenersi effettivamente libero. Pertanto affinché il consenso al trattamento biometrici risulti libero è necessario che l'interessato abbia la possibilità di ricorrere eventualmente ad una sua valida alternativa, come ribadito recentemente anche dall'EDPB nelle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video[105]. Tuttavia, non sempre è possibile ricorrere a forme di autenticazione meno intrusive. Nel caso di sistemi di autenticazione basati sul riconoscimento biometrico per accedere a settori dell'azienda ad alto rischio o autorizzare l'impiego di macchinari pericolosi che richiedono un'elevata esperienza

[103] M. Martorana, *Trattamento dei dati biometrici e utilizzi in ambito commerciale*, in *Altalex*, 18 febbraio 2021.
[104] Gruppo Art. 29, Parere 2/2017 sul trattamento dei dati sul posto di lavoro, adottato l'8 giugno 2017 WP249.
[105] EDPB, Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 10 luglio 2019.

professionale, l'uso di uno strumento alternativo avrebbe un impatto estremamente significativo sulle misure di sicurezza aziendali, che ne risulterebbero indebolite. Inoltre, se fosse ammesso il ricorso a forme alternative di autenticazione in questi contesti ad alto rischio verrebbero a mancare i presupposti che giustificano il ricorso ai dati biometrici, qualificando il ricorso a questa tipologia di dati come una misura sproporzionata. Il bilanciamento fra le esigenze di sicurezza aziendali e la tutela dei diritti dei lavoratori può essere ulteriormente perfezionato dalle elaborazioni giurisprudenziali dei singoli Stati membri.

Come vedremo all'interno del secondo capitolo, ad esempio, il Garante italiano per la protezione dei dati personali ha escluso categoricamente l'uso di sistemi di riconoscimento biometrico per la rilevazione degli accessi sul luogo di lavoro. Nel nostro ordinamento il trattamento di dati biometrici per finalità di ordinaria gestione del rapporto di lavoro non viene ritenuto ammissibile, in quando potendo essere raggiunta la medesima finalità attraverso mezzi di identificazione meno intrusivi l'uso di questi sistemi risulta sproporzionato. Questo orientamento era già emerso dall'affermazione del principio di necessità all'interno del parere 3/2012 del WP29, il quale impone di verificare se la finalità perseguita dal trattamento di dati biometrici non possa essere realizzata utilizzando dati che non coinvolgano il corpo.

4.3 Il trattamento di dati biometrici da parte di Autorità di pubblica sicurezza

L'adozione del regolamento generale sulla protezione dei dati (UE) 2016/679 è stata accompagnata dalla previsione di una direttiva che predisponesse delle misure chiare per la tutela delle persone fisiche in riferimento al trattamento di dati personali da parte di autorità pubbliche, per fini di prevenzione, indagine e perseguimento di reati. La direttiva (UE) 2016/680[106] nasceva dall'esigenza nei settori della cooperazione di polizia e della cooperazione giudiziaria in materia penale di assicurare un livello uniforme ed elevato di protezione dei dati personali delle persone fisiche, agevolando al contempo lo scambio di dati personali tra le autorità competenti degli Stati membri, per garantire una maggiore efficacia giudiziaria in materia penale e di polizia[107]. La direttiva è entrata in vigore il 5 maggio 2016 ed è stata attuata il 6 maggio 2018. All'interno del testo della suddetta direttiva, il divieto generale di trattamento dei dati biometrici per l'identificazione univoca di una persona fisica sancito all'art. 9, par. 1 GDPR non viene applicato in tre contesti: nella prevenzione e nella lotta contro la criminalità o nell'esecuzione di sanzioni; nei casi in cui sia necessario prevenire

[106] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, del 27 aprile 2016, in G.U.U.E. L 119/89.
[107] Ivi, nota 87 (considerando 7).

o salvaguardare minacce alla pubblica sicurezza e purché i dati siano trattati dalle Autorità competenti (ai sensi dell'art. 3, par. 7 della direttiva)[108]. Inoltre queste Autorità sono autorizzate a predisporre il trattamento di dati biometrici con finalità di identificazione univoca solo se le tre condizioni cumulative definite all'art. 10 (trattamento di categorie particolari di dati personali) sono rispettate. In particolare il trattamento è ammesso solo:

- se *strettamente necessario*
- e se soggetto ad *adeguate garanzie* per i *diritti* e le *libertà* delle persone interessate
- e solo:
  a) se autorizzato dal diritto dell'Unione o dello Stato membro;
  b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o
  c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato.

In presenza di un quadro giuridico chiaro ed un uso proporzionato di questi sistemi, si è sempre ritenuto fondamentale garantire alle autorità di polizia l'accesso a queste tecnologie in funzione della tutela della pubblica sicurezza. L'accesso a immagini facciali, impronte digitali o altri dati biometrici, se configurato all'interno di un'esigenza di interesse pubblico si può ritenere un'ingerenza necessaria nella vita delle persone per consentire di individuare e perseguire crimini, identificare sospetti e agevolare indagini giudiziarie. Tuttavia, in più occasioni la Corte europea dei diritti dell'uomo si è pronunciata in merito ribadendo come già solo la semplice raccolta e memorizzazione di dati personali da parte di pubbliche autorità interferisca ampiamente nelle garanzie a tutela della vita privata dei soggetti interessati, anche senza che sia esercitato un uso successivo di tali dati[109].
Anche se questi dati non sono necessariamente impiegati in funzioni di controllo una volta acquisiti, la loro raccolta e conservazione può costituire un'interferenza sproporzionata con il diritto alla vita privata delle persone, tanto più se sottoposti a forme di trattamento automatizzate e conservati in database di polizia. Per questo si rende necessario vincolare il trattamento di dati biometrici per indentificare in modo univoco un soggetto al principio di necessità, con garanzie specifiche ed un quadro giuridico ben definito. Altrimenti la conservazione di dati biometrici e l'interferenza di questi sistemi con i diritti fondamentali esporrebbero le persone ad una forte vulnerabilità verso i pubblici poteri. Spetta pertanto al diritto nazionale dei singoli Stati membri regolamentare dettagliatamente la registrazione e la conservazione di questi dati per scopi di identificazione biometrica da parte di autorità pubbliche. Ad oggi una regolamentazione accurata sulla conservazione dei dati biometrici

[108] E. J. Kindt, *Having yes, using no? Abaout the new legal regime for biometric data*, cit., p. 527.
[109] ECtHR, S. and Marper v. United Kingdom, nos. 30562/04 and 30566/04, 4 Dicember 2008.

risulta ancora prevalentemente assente nel diritto nazionale degli Stati europei, nonostante l'esponenziale aumento della creazione di queste banche dati ed il rischio crescente di una loro raccolta senza una chiara base legale.

Un altro fattore di rilievo riguarda l'accesso da parte di autorità di pubblica sicurezza alle banche dati detenute da attori privati[110], con il conseguente utilizzo dei dati per i fini perseguiti da queste autorità, quando le finalità di raccolta iniziali con cui si era provveduto alla creazione di queste banche dati erano ben diverse. Si tratta di un fenomeno definito da E. J. Kindt come "a growing biometric crowd of suspects"[111] (un crescente agglomerato biometrico di sospetti), in quanto le autorità nazionali di pubblica sicurezza ottengono in questo modo anche l'accesso a banche dati contenenti pure dati appartenenti a cittadini non europei. Queste operazioni consentono alla polizia di effettuare procedure di cyber-sicurezza identificando gli individui attraverso database biometrici globali detenuti da soggetti terzi. Al momento non esiste un progetto di legislazione europeo che consenta l'accesso a database di cittadini europei, come ad esempio le banche dati per la raccolta delle identità personali, ma non è escludibile che ciò possa avvenire in un prossimo futuro.

Anche la rilevazione di immagini all'interno di spazi pubblici per finalità di pubblica sicurezza risulta problematica, in quanto la registrazione ininterrotta e in tempo reale dei cittadini implicherebbe provvedere ad una loro profilazione senza i presupposti di un sospetto individualizzato e senza un mandato, come avviane invece nei database di polizia per i soggetti condannati o arrestati. In questi casi ogni soggetto all'interno di uno spazio pubblico viene potenzialmente ritenuto un sospetto, oltretutto attraverso delle forme di rilevazione spesso invisibili e di cui il soggetto non è a conoscenza. Intervenendo a questo proposito, infatti, il 6 ottobre 2021 il Parlamento europeo ha approvato a maggioranza una risoluzione con cui ha esortato la Commissione europea a proibire con un atto normativo generale, l'uso del riconoscimento facciale come misura di sorveglianza all'interno degli spazi pubblici dell'Unione europea[112].

L'obiettivo della risoluzione[113] consiste nel vietare l'uso del riconoscimento facciale all'interno degli spazi pubblici da parte delle forze di polizia. Il Parlamento ha richiesto dunque espressamente che la regolazione del settore escluda all'interno di qualsiasi spazio pubblico ogni forma di trattamento di dati biometrici, a partire dalle immagini facciali. Viene inoltre richiesta l'interruzione dei finanziamenti per la ricerca biometrica, chiedendo di limitare lo sviluppo di sistemi biometrici che

[110] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* cit., p. 354-357.
[111] E. J. Kindt, *Having yes, using no? Abaout the new legal regime for biometric data*, cit., p. 528.
[112] S. Bocconetti, *L'europarlamento contro la sorveglianza di massa nei luoghi pubblici*, in *Il Manifesto*, 6 ottobre 2021. https://ilmanifesto.it/leuroparlamento-contro-la-sorveglianza-di-massa-nei-luoghi-pubblici/
[113] Parlamento europeo, Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale (2020/2016(INI)) P9_TA(2021)0405.

possano contribuire a forme di sorveglianza indiscriminata all'interno degli spazi pubblici. Questa risoluzione si inserisce all'interno del dibatto in merito alla proposta di Regolamento sull'Intelligenza Artificiale[114] presentata il 21 aprile 2021, che dovrà essere approvato dalla Commissione europea. I prossimi mesi risulteranno cruciali per determinare se la Commissione adotterà l'orientamento indicato dall'europarlamento.

4.4 Il trattamento di dati biometrici da parte di istituzioni, organi, uffici e agenzie europee

Come già analizzato all'interno del secondo paragrafo di questo elaborato, all'art 2, par. 3 del GDPR si stabilisce che per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione sia applicato il Regolamento (CE) n. 45/2001. Inoltre il medesimo paragrafo impone ai legislatori europei l'adeguamento del testo del Regolamento n. 45/2001 CE alle previsioni introdotte dal GDPR. Ciò è avvenuto con l'approvazione del Regolamento UE n. 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, che ha abrogato definitivamente il Regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

Questo Regolamento introduce delle norme a tutela delle persone fisiche in relazione al trattamento dei dati personali dei cittadini europei effettuati da parte delle istituzioni e degli organi dell'Unione. Esso regola inoltre la libera circolazione dei dati personali tra più istituzioni e organi o verso altri destinatari all'interno del territorio europeo. In esso viene affidato all'EDPS la sorveglianza sulla corretta applicazione delle disposizioni del regolamento in ogni trattamento effettuato da un'istituzione o organo europeo. Si tratta dell'ultimo tassello a completamento del rinnovo della disciplina sulla protezione dei dati personali posto dall'approvazione del GDPR e della Direttiva 2016/680 sui trattamenti effettuati da Autorità di pubblica sicurezza.Questo quadro risulterà ancora maggiormente efficace quando sarà resa effettiva l'introduzione del Regolamento sulla E-Privacy[115], l'atto normativo che dovrebbe abrogare e sostituire il testo della direttiva 2002/58/CE. Il 10 febbraio 2021 il Consiglio Europeo ha approvato un testo sull'E-Privacy che dovrà essere oggetto di confronto con il Parlamento europeo.

[114] Proposta di Regolamento del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'Intelligenza Artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM/2021/206 final.

[115] Il 10 gennaio 2017 è stata presentata la proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettriniche) COM/2017/010 final – 2017/03 (COD).

5. Ulteriori sviluppi nel diritto europeo in materia

In ultima analisi possiamo ravvisare al momento in cui si scrive due ultimi significativi sviluppi nel diritto europeo nell'ambito della regolamentazione dei sistemi biometrici. Attualmente attraverso la pubblicazione della proposta di Regolamento sull'Intelligenza Artificiale e la riforma in atto della disciplina del Regolamento eIDAS, possiamo determinare come l'orientamento generale del legislatore europeo in materia di biometria si stia spostando verso una regolazione più estensiva di questo mercato e delle restrizioni più stringenti. Ciò, come già evidenziato, è emerso anche in recenti risoluzioni adottate dal Parlamento Europeo per introdurre delle restrizioni nell'utilizzo di sistemi di identificazione biometrica all'interno di spazi pubblici come misure di sicurezza. Di seguito analizzeremo in dettaglio le novità che saranno introdotte attraverso queste due riforme.

5.1 Intelligenza artificiale e riconoscimento biometrico

Il 21 aprile 2021 la Commissione europea ha pubblicato la proposta di Regolamento sull'approccio europeo all'Intelligenza Artificiale[116]. Questa proposta si inserisce all'interno della strategia europea per la definizione di un primo quadro giuridico sull'IA, che risulti uniforme all'interno dell'Unione. In esso viene posta un'analisi dei rischi connessi all'utilizzo di questi sistemi, con la finalità tutelare i diritti fondamentali e la sicurezza degli utenti europei coinvolti e si prevede inoltre l'adozione di un nuovo piano coordinato sull'Intelligenza Artificiale 2021[117] volto a rafforzare gli investimenti e finanziare l'innovazione nel settore[118]. La proposta di Regolamento predispone in generale l'armonizzazione delle regole di trasparenza applicabili a tutti i sistemi di intelligenza artificiale e prevede una disciplina speciale più garantista per i sistemi di IA definiti come ad "alto rischio", per i quali vengono stabiliti obblighi specifici. All'interno del Titolo II dedicato alle pratiche di intelligenza artificiale vietate, l'art. 5 sancisce che non sono ammissibili i sistemi di IA che prevedano:

a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne

[116] COM (2021) 206 final.
[117] Commissione europea, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comunitato delle regioni, *"Promuovere un approccio europeo all'intelligenza artificiale"* COM (2021) 205 final.
[118] Camera dei deputati, Documentazione parlamentare *"Il nuovo approccio europeo all'Intelligenza Artificiale"*, Studi – trasporti, 22 aprile 2021.

materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;

b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;

c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari:

   i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;

   ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;

Alla lettera d) poi troviamo un'esplicita menzione dei sistemi di identificazione biometrica all'interno di spazi pubblici come pratica di intelligenza artificiale espressamente vietata, salvo alcune eccezioni ivi individuate:

d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:

   i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi;

   ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;

   iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro.

Lo stesso paragrafo 2 dell'art. 5 specifica ulteriormente questa misura predisponendo che l'uso dei sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico per attività di contrasto, tenga conto deve tener conto di due elementi:

a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno causato dal mancato uso del sistema;
b) le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze.

Inoltre devono essere garantite anche il rispetto delle tutele delle condizioni necessarie e proporzionate in relazione all'uso, in particolare per quanto concerne le limitazioni temporali, geografiche e personali.

All'interno del Titolo III dedicato ai sistemi di IA classificati come ad alto rischio, l'art. 6, paragrafo 1 stabilisce le regole alla base di questa classificazione. Un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe queste condizioni:

a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II;
b) il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II.

Il secondo paragrafo dell'art. 6, stabilisce che oltre ai sistemi di IA classificati sula base di queste due condizioni, anche i sistemi di IA individuati all'interno dell'allegato III siano considerati come ad alto rischio. Non a caso all'interno di questo elenco individuiamo all'interno del primo punto proprio i sistemi di identificazione e categorizzazione biometrica delle persone fisiche, definiti come i sistemi di IA destinati a essere utilizzati per l'identificazione biometrica remota "in tempo reale" e "a posteriori" delle persone fisiche[119]. Come abbiamo ricostruito la disciplina della proposta di Regolamento sull'IA interviene notevolmente nella disciplina dei sistemi di identificazione biometrica. Anzitutto l'utilizzo di questi sistemi con finalità di contrasto viene espressamente vietata

[119] Allegato III, Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2, settore 1.

all'interno degli spazi europei, salvo alcuni usi specifici definiti espressamente. È significativo a questo proposito rilevare come la risoluzione adottata dal Parlamento europeo il 6 ottobre 2021 sia intervenuta proprio su questo punto per richiedere espressamente un divieto generale dell'utilizzo di questi sistemi negli spazi pubblici, escludendo pure i casi specifici ammessi ai sensi dell'art. 5, par. 1, lett d). Inoltre, in generale i sistemi di identificazione e categorizzazione biometrica delle persone fisiche sono sempre classificati come sistemi di intelligenza artificiale ad alto rischio, attribuendo alla loro disciplina la definizione di requisiti specifici (art. 8), di sistemi per l'apposita gestione dei rischi (art. 9), delle previsioni specifiche sulla governance dei dati (art. 10), sulla conservazione delle registrazioni (art. 12), sulla trasparenza e fornitura di informazioni agli utenti (art. 13) e da ultimo, delle limitazioni specifiche relative all'impiego di questi sistemi in attività di sorveglianza umana (art. 14). Pertanto possiamo determinare come la proposta di Regolamento segua un vero e proprio piano di modernizzazione della disciplina europea in campo biometrico, focalizzandosi in particolare sull'uso a fini identificatori di questi sistemi. L'approccio così codificato dal legislatore europeo si configura come un metodo più votato ad uso etico di queste tecnologie ormai imprescindibili nel nostro quotidiano. In conclusione, all'interno questo mosaico giuridico di cui questo regolamento costituirà l'ultimo tassello si vuole non solo favorire le opportunità che l'IA offre per le istituzioni, ma anche valutare approfonditamente i rischi e le responsabilità che i fornitori di beni e servizi dovranno assumersi all'interno di questo settore.

5.2 Identità digitale e riconoscimento biometrico

La proposta di revisione del regolamento eIDAS[120] è stata presentata dalla Commissione europea il 3 giugno 2021. Il regolamento (UE) n. 910/2014[121] sull'identità digitale è stato introdotto con l'obbiettivo di ideare una normativa comunitaria per i servizi fiduciari e i mezzi di identificazione elettronica all'interno dell'Unione[122]. Da mesi attualmente è in corso una sua revisione rispetto alla normativa in materia di identificazione digitale. L'obiettivo della riforma è di estendere la disciplina europea in merito attraverso misure specifiche e riducendo gli spazi di discrezionalità attribuite agli Stati membri per la sua attuazione. Uno dei profili più innovativi della riforma riguarda l'ideazione

[120] Relazione della commissione al Parlamento europeo e al Consiglio sulla valutazione del regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), Commissione europea, COM (2021) 290 final, 3 giugno 2021.
[121] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE in G.U.U.E. L 257/73.
[122] AGID, pagina dedicata al Regolamento eIDAS.
https://www.agid.gov.it/it/piattaforme/eidas

di un *European Digital Identity Wallet* per l'identificazione elettronica[123]. Queste specie di "portafogli" digitali dovranno contenere i dati di identificazione e le credenziali elaborate per consentire l'accesso del cittadino ai servizi digitali offerti dalle istituzioni comunitarie ed effettuare transazioni transfrontaliere all'interno dell'Unione. Il rilascio dei wallet digitali però sarà regolato in modo specifico da ciascun Stato membro, che potrà pure avvalersi della collaborazione di un soggetto terzo. Questo pone delle questioni critiche in merito al tipo di garanzie offerte per la raccolta di questi dati personali, dato che il margine di autonomia offerto a ciascuno stato sembra essere molto ampio attualmente. In ogni caso viene imposto un livello di sicurezza elevato per il trattamento di questi dati ai sensi dell'art. 8 del regolamento eIDAS.

Necessariamente in queste previsioni il rilascio di documenti di identificazione resta una prerogativa unicamente statuale, ma la riforma si prefigge l'obiettivo di agevolare l'utilizzo e l'interoperabilità a livello europeo di forme di identificazione digitale. All'interno di questo ambito si inserisce contestualmente pure il dibattito sull'utilizzo di dati biometrici, in quanto ogni documento di identità predispone alla sua base la raccolta di un dato biometrico sotto forma di foto identificativa del soggetto. Sia la carta d'identità che il passaporto vedono incorporata al loro interno l'immagine del volto del loro titolare, ciò avviene anche nel loro formato elettronico riconosciuto in tutta Europa ai sensi del Regolamento (UE) 2019/1157[124] e Regolamento (CE) n. 2252/2004[125]. Il formato elettronico di questi documenti garantisce elevate misure di sicurezza proprio grazie alla sua natura biometrica e informatica. Inoltre gli Stati membri hanno l'obbligo di inserire all'interno del passaporto elettronico pure le impronte digitali dell'indice della mano destra e della mano sinistra, per agevolare le misure sicurezza nei viaggi oltre le frontiere europee e garantire una rapida interoperabilità fra i sistemi di polizia dei vari stati. I documenti d'identità pertanto si distinguono dai meri strumenti di identificazione elettronica (quali badge o password) per la compresenza di tre elementi: la rilevazione di un dato biometrico (quali immagini facciali, impronte digitali), la competenza per il rilascio esclusiva da parte dello Stato e l'obbligatorietà nella dotazione e nell'utilizzo[126]. L'incorporazione del dato biometrico all'interno di questi documenti diventa una misura essenziale, poiché solo attraverso la sua ispezionabilità diretta da parte da parte di un funzionario autorizzato si può verificare la corretta appartenenza del documento al suo titolare. Vi sono di fatto usi dell'identità digitale che

[123] Comunicato stampa del 3 giugno 2021, *Proposta della Commissione relativa a un'identità digitale affidabile e sicura per tutti gli europei.*

[124] Regolamento (UE) 1157/2019 del Parlamento europeo e del Consiglio del 20 giugno 2019 sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione, in G.U.U.E. L 188/67.

[125] Regolamento (CE) 2252/2004 del Consiglio del 13 dicembre 2004 relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri in G.U.C.E. L 385.

[126] Nel nostro Stato non sono ammessi cittadini senza il possesso di una carta d'identità; per viaggiare in paesi extra europei il passaporto è il documento di riconoscimento obbligatorio.

rendono obbligatorie forme di identificazione ufficiali di questo tipo, come avviene per esempio nell'ambito di contratti vincolati predisposti online o in sede giurisdizionale nel caso di un intervento da remoto di un testimone o di una delle parti[127].

[127] E. Tosi, *Diritto privato delle nuove tecnologie digitali, Riservatezza, contratti, responsabilità tra persona e mercato*, in *Diritto delle nuove tecnologie*, Giuffrè Francis Lefevbre, 2021, p. 423-439.

CAPITOLO 2: I DATI BIOMETRICI NELL'ORDINAMENTO ITALIANO

"Il tema della sorveglianza (…) assume così importanza essenziale, poiché risulta ormai evidentissimo che il futuro delle nostre organizzazioni sociali sarà fortemente condizionato, da una parte, dal modo in cui verranno impiegate le diverse e sempre più sofisticate tecnologie di controllo e, dall´altra, dalla qualità dei dati raccolti, tra i quali spiccano per delicatezza quelli genetici e, più in generale, quelli biometrici. (…) È pure il nostro modo di vivere in pubblico ad essere influenzato, cambia il modo in cui percepiamo e viviamo la nostra stessa libertà. È troppo dire che si è ovunque aperta una ***nuova****, e* ***inedita****,* ***questione democratica****?*[128] *"*

(Stefano Rodotà, 2001)

1. L'evoluzione del dibattito italiano sui dati biometrici

Analogamente a quanto tracciato nel primo capitolo per la disciplina europea, pure il nostro legislatore stentava inizialmente a riconoscere una disciplina giuridica del dato biometrico. I motivi del ritardo italiano nello sviluppo di questa disciplina sono vari, da un lato il nostro paese ha preso coscienza del fenomeno molto tardi, giudicandolo secondario e prematuro, dall'altro per molto tempo nel settore informatico è mancata un'adeguata politica di controllo e coordinamento[129].
Nel nostro ordinamento gli albori della normativa italiana in materia di tutela dei dati personali sono da ricondurre alla legge n. 675/1996[130], che recepiva la direttiva 95/46/CE, e al successivo riordino della materia avvenuto con la pubblicazione del Codice della privacy, con il d.lgs. n. 196/2003[131]. In realtà, sebbene mancasse una chiara definizione giuridica, alcuni aspetti relativi al trattamento di dati biometrici e al loro impatto sui diritti e le libertà fondamentali dei cittadini erano già presenti nel dibattito in dottrina. In particolare, due previsioni interne al Codice privacy richiamavano

[128] Discorso del professor Rodotà di presentazione della Relazione per l'anno 2001, Garante per la protezione dei dati.
[129] G. Gardini, *Le regole dell'informazione, l'era della post-verità,* Torino, G. Giappichelli Editore, 2017 pag. 295-297.
[130] Legge n. 675 del 31 dicembre 1996, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, testo consolidato con il d.lg. 28 dicembre 2001, n. 467, pubblicata sulla Gazzetta Ufficiale n.5 dell'8 gennaio 1997 – Suppl. Ord. n. 3 (legge abrogata ai sensi dell'art. 183, comma 1, lett a) del Codice in materia dei dati personali.
[131] Codice in materia di dati personali, d.lgs. 30 giugno 2003, n. 1996, pubblicato in Gazzetta Ufficiale n. 174 del 29 luglio 2003 – Suppl. Ord. n. 123.

direttamente l'utilizzo di dati biometrici[132]. La prima riguardava l'art. 37, comma 1, lett. a) del Codice, relativo agli adempimenti in materia di notificazione del trattamento. In esso si prevedeva l'obbligo di notifica del trattamento da parte del titolare al Garante privacy, se il trattamento includeva dati genetici, biometrici o dati che indicassero la posizione geografica di persone o oggetti mediante una rete di comunicazione elettronica.

L'introduzione di un obbligo di notificazione era giustificata dall'esigenza di garantire un maggior controllo e trasparenza per queste tipologie di trattamento, data la natura peculiare dei diritti degli interessati e dei rischi connessi all'utilizzo di questi dati. All'interno invece dell'art. 55 del Codice, relativo all'impiego di particolari tecnologie, si stabiliva che il trattamento di dati personali che implicasse maggiori rischi per l'interessato, quali l'utilizzo di banche di dati genetici o biometrici, dovesse essere effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17 e sulla base di preventiva comunicazione ai sensi dell'articolo 39.

L'art. 17 del Codice svolgeva un ruolo essenziale regolando le forme di trattamento che presentassero dei rischi specifici per i diritti e le libertà fondamentali, nonché la dignità dell'interessato, le quali erano ammesse solo nel rispetto delle misure di garanzia e degli accorgimenti prescritti dal Garante in applicazione dei principi del Codice. Le misure e gli accorgimenti, di cui al comma 1 dell'art. 17, erano prescritti dal Garante in applicazione dei principi sanciti dal Codice e nell'ambito di una verifica preliminare all'inizio del trattamento.

Ognuno di questi articoli è stato in seguito abrogato con l'introduzione del decreto di adeguamento al Regolamento (UE) 679/2016, ma è interessante partire da essi per introdurre l'evoluzione della disciplina italiana sui dati biometrici. La loro adozione ci mostra come la normativa italiana inizialmente pur evitando di identificare esplicitamente i dati biometrici come categorie di dati sensibili, ne riconoscesse già alcune peculiarità adottando delle misure di garanzia specifiche. In particolare fu il legislatore italiano, anticipando quello europeo, a introdurre per i dati biometrici il procedimento di garanzia della verifica preliminare (c.d. *prior checking*)[133], come vedremo in dettaglio. Un ruolo essenziale nell'orientare le riflessioni in dottrina sulla biometria è stato ricoperto dal Garante italiano per la protezione dei dati personali. Il nostro Garante già a partire dal 2000, come testimonia il discorso dell'allora presidente Rodotà citato all'inizio di questo capitolo, poneva l'accento sui sistemi di riconoscimento biometrico e l'esigenza di porre una loro regolazione. Trattando delle nuove frontiere della biometria e del loro mercato in espansione, si sottolineava l'emersione di una "nuova e inedita questione democratica". La diffusione di sistemi di controllo basati su dati biometrici, giustificata da generiche ragioni di sicurezza, poneva questioni fino ad allora

[132] R. Ducato, *I dati biometrici*, cit., p. 1296-1297.
[133] F. Di Resta, *La nuova "Privacy europea", i principali adempimenti del regolamento UE 2016/679 e profili risarcitori,* G. Giappichelli Editore, 2018, p. 20.

inedite sul rapporto fra diritti e libertà dei cittadini e il loro bilanciamento con il perseguimento del bene pubblico. "*Più controllo, più libertà*" affermava sinistramente uno degli slogan propagandistici all'inizio di 1984 di Gorge Orwell, citato nel discorso del professore: una realtà distopica che per certi versi non si prefigurava più così lontana[134]. Per questo iniziarono a porsi riflessioni in dottrina su come elaborare un sistema di regole adeguato all'utilizzo di questi sistemi. Di fatto, proprio attraverso l'attività del Garante per la privacy abbiamo iniziato ad applicare la disciplina per la tutela dei dati personali ai sistemi biometrici nel nostro paese.

Già da prima dell'introduzione del Codice della privacy, attraverso la disciplina posta dalla legge n. 675/1996, il Garante era intervenuto in più settori regolando ad esempio le modalità di raccolta di impronte digitali all'ingresso di istituti bancari, di credito o di locali privati e fissando alcuni criteri di base[135]: l'adozione di metodi alternativi di identificazione per chi non volesse acconsentire al trattamento dei propri dati biometrici; la raccolta dei dati attraverso modalità criptate; un'indicazione temporanea della loro conservazione (es. una settimana); l'accesso ai dati solo da parte di autorità di polizia o magistratura; nonché il rispetto del principio di necessità e del principio di proporzionalità, accertando se la finalità perseguita non possa essere realizzata utilizzando mezzi alternativi.

Con l'approvazione del d.lgs. n. 196/2003 e la diffusione del Documento di lavoro sulla biometria del Gruppo Art. 29 nel medesimo anno, si ottiene un primo corpus normativo che estende al trattamento di dati biometrici la disciplina per la tutela dei dati personali e adotta le misure sull'informativa e il consenso[136]. Sulla base di questi principi l'interessato forniva il suo consenso al trattamento solo dopo aver acquisito dettagliatamente l'informativa sul trattamento, che ne definiva le finalità, il periodo di conservazione dei dati, i diritti dell'interessato e la possibilità di limitare l'utilizzo di dati tali per ulteriori scopi una volta raccolti.

Il Garante per la privacy, oltre a svolgere un'attività di integrazione e vigilanza di queste misure attraverso l'adozione di autorizzazioni, pareri, prescrizioni e in alcuni casi divieti e sanzioni, spesso ha influito notevolmente anche nell'ambito della politica legislativa, contribuendo all'elaborazione di proposte di legge, come nell'ambito dei lavori parlamentari della legge n. 189/2002 in materia di

---

[134] Discorso del professor Rodotà di presentazione della Relazione per l'anno 2001, Garante per la protezione dei dati. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3541955

[135] Garante per la protezione dei dati personali, *Videosorveglianza e biometria – Trattamento dati personali mediante l'utilizzo di impronte digitali,* 19 novembre 1999 (doc. web. 42058); ID., *Videosorveglianza – Impronte digitali per l'accesso in banca*, 11 dicembre 2000 (doc. web. 30903); ID., *Videosorveglianza e rilevazione di impronte digitali all'ingresso di banche*, 28 febbraio 2001 (doc. web. 40181); ID., *Raccolta di impronte digitali associate ad immagini per l'accesso a banche*, 7 marzo 2001 (doc. 30947); ID., *Videosorveglianza e dati biometrici – Rilevazioni biometriche presso istituti di credito,* 28 settembre 2001 (doc. 39704); ID., Permesso di soggiorno elettronico, 15 ottobre 2003 (doc. web. 1054786).

[136] A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici*, in S. Scagliarini (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali, la normativa italiana dopo il d.lgs. n. 101/2018*, Collana Fondazione Marco Biagi, G. Chiapparelli Editore, 2019, p. 119.

immigrazione d'asilo[137], che ha introdotto una rilevazione biometrica per i soggetti immigrati che richiedano il permesso di soggiorno o il suo rinnovo[138]. Inoltre negli anni successivi, l'attenzione del Garante verso i sistemi di riconoscimento biometrico ha continuato a mantenersi alta, specialmente in riferimento all'adozione di tali sistemi per la regolazione dell'accesso a luoghi di lavoro, ad istituti scolastici e servizi quali le mense, come sarà approfondito nei prossimi paragrafi[139]. Tuttavia, il ruolo del Garante nella definizione della disciplina biometrica si rivela essenziale con l'adozione del Provvedimento generale prescrittivo in tema di biometria emanato nel novembre 2014[140].

Il Provvedimento approvato dopo l'indizione di una consultazione pubblica[141], per acquisire contributi da parte di ricercatori e sviluppatori di questi sistemi, aveva l'obiettivo di semplificare la regolazione delle tecnologie biometriche, stipulando delle procedure chiare e rigorose a cui i soggetti pubblici e privati fossero obbligati ad attenersi scrupolosamente. Al suo interno l'Autorità individuava alcuni casi specifici nei quali non era più necessario attenersi alla richiesta di verifica preliminare per l'adozione di tecnologie biometriche, definendo diametralmente uno speculare sistema di garanzie a tutela delle libertà personali. Veniva concesso pertanto il rilevamento delle impronte digitali per l'accesso fisico ad aree riservate e l'uso della topografia della mano per usi facoltativi quali l'accesso a banche e biblioteche, solo se in presenza del consenso espresso degli interessati e purché fossero contestualmente garantite delle forme alternative di autenticazione senza il ricorso a dati biometrici.

Inoltre, attraverso l'adozione di apposite linee guida, veniva concesso anche l'utilizzo della firma grafometrica per la sottoscrizione di documenti informatici, mentre veniva esclusa categoricamente la possibilità di realizzare archivi biometrici centralizzati o l'utilizzo dei dati per finalità diverse da quelle indicate dal consenso dell'interessato[142]. Il Provvedimento generale, sotto l'influenza del parere 3/2012 sugli sviluppi delle tecnologie biometriche elaborato dal Gruppo Art. 29, ne riprendeva la medesima descrizione raffigurando i dati biometrici come "proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali

[137] Legge n.189 del 30 luglio 2002, Modifica alla normativa in materia di immigrazione e di asilo, pubblicata sulla Gazzetta Ufficiale il 26 agosto 2002 – Suppl. Ord. n. 173.

[138] Garante per la protezione dei dati personali, *Stato di attuazione della legge n. 675/1996 – Le principali novità sul piano normativo, Relazione 2002*, 20 maggio 2003, par. 2, lett. g) e i).

[139] Garante per la protezione dei dati personali, *Trattamento di dati biometrici per la verifica della presenza dei dipendenti e l'accesso ad aree produttive (mulino)*, 15 giugno 2006 (doc. web. 1306530); ID., *Sistema di firma elettronica avanzata grafometrica. Verifica preliminare*, 4 giugno 2015 (doc. web. 4172308); ID., *Sistema biometrico basato sul trattamento di impronte digitali per finalità di rilevazione delle presenze dei dipendenti di un Comune*,17 marzo 2016 (doc. web. 4948405).

[140] Garante per la protezione dei dati personali, *Provvedimento generale prescrittivo in materia di biometria*, 12 novembre 2014, in G.U. 2 dicembre 2014 n. 280 (doc. web. 3556992).

[141] ID., *Avvio della consultazione su Provvedimento e Linee guida in tema di riconoscimento biometrico e firma grafometrica*, in G.U. 23 maggio 2014, n. 118.

[142] Garante per la protezione dei dati personali, *Biometria: il Garante detta le nuove regole e apre una consultazione*, comunicato stampa del 26 novembre 2014 (doc. web. 3129762).

caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità" e ne confermava la natura peculiare, sottoponendo il loro trattamento all'obbligo di notificazione di qualsiasi violazione o irregolarità informatica (c.d. data breach)[143]. Oltre al Provvedimento generale erano state sottoposte a consultazione pubblica anche le Linee guida in tema di riconoscimento biometrico e firma grafometrica[144] contenute all'interno dell'allegato A, parte integrante del medesimo documento, abbreviate "Linee guida Biometria". Il loro obiettivo era definire un quadro più puntuale di queste tecnologie, cristallizzando alcuni principi che caratterizzeranno in seguito la materia[145]. Al punto 4.1 delle linee guida, infatti, veniva sancito il *principio di liceità* e *correttezza* del trattamento dei dati biometrici, mentre il *principio di necessità* era definito all'interno del punto 4.2, che imponeva di verificare se le medesime finalità del trattamento non potessero essere raggiunte attraverso modalità meno invasive che non richiedessero la rilevazione di dati biometrici. Inoltre, nei casi in cui il ricorso a tecniche biometriche risultasse irrinunciabile, quest'ultimo doveva comunque essere attuato nel minor tempo possibile. Il punto 4.3 prevedeva il principio di finalità, stabilendo che i dati raccolti e processati attraverso tecniche biometriche fossero utilizzati solo per le finalità stabilite per la loro raccolta e da ultimo, il punto 4.4 riguardava il principio di proporzionalità, secondo il quale il trattamento può coinvolgere solo i dati strettamente necessari in relazione alle finalità perseguite. Inoltre, se il sopra citato principio generale dell'istanza di verifica preliminare (c.d. "prior checking"), modificato dal Provvedimento nell'ambito della regolazione dei dati biometrici, era regolato all'interno dell'art. 17 del Codice della privacy citato all'inizio di questo paragrafo, nelle Linee guida Biometria al punto 4.5.3 si disponeva che l'istanza di verifica dovesse indicare:

- la tipologia di dati biometrici trattati;
- il contesto e le specifiche finalità perseguite mediante il sistema biometrico che si intende installare;
- le ragioni in base alle quali si ritengono inidonei rispetto agli scopi perseguiti sistemi alternativi che pongono minori rischi per i diritti e le libertà fondamentali degli interessati;
- le modalità di funzionamento del sistema nonché le modalità di acquisizione, utilizzo e archiviazione dei dati biometrici e la durata della loro eventuale conservazione;

[143] A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici,* cit., p. 117.
[144] Garante per la protezione dei dati personali, *Linee guida in materia di riconoscimento biometrico e firma grafometrica*, Allegato A al provvedimento del Garante del 12 novembre 2014 (doc. web. 3563006).
[145] G. Bellomo, *Biometria e digitalizzazione della pubblica amministrazione,* in S. Civitarese Matteucci, L. Torchia (a cura di), *La tecnificazione,* Vol. 4, Firenze University Press, 2016, p. 65-66.

- l'eventuale idoneità del dato biometrico raccolto a rivelare informazioni relative allo stato di salute degli interessati;
- gli eventuali vantaggi per gli interessati e per i titolari del trattamento derivanti dall'utilizzo di dati biometrici;
- i rischi individuati e gli accorgimenti tecnici e organizzativi messi in atto per mitigarli;
- le modalità di acquisizione del consenso, ove previsto, i sistemi alternativi, il testo dell'informativa

Inoltre, nell'istanza di verifica predisposta dal titolare doveva essere anche indicata l'analisi dei rischi effettuata e le modalità adottate per garantire le misure di carattere generale applicabili ai trattamenti di dati biometrici[146]. Il Garante, tuttavia, individuava anche alcune tipologie specifiche di trattamento di dati biometrici a rischio ridotto per le quali veniva escluso l'obbligo di verifica preliminare, a condizione che venissero rispettati tutti i presupposti di legittimità stabiliti all'interno del Codice e delle medesime linee guida. I trattamenti esonerati dall'obbligo di presentare la richiesta di verifica preliminare concernevano l'autenticazione informatica; il controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e l'utilizzo di apparecchi e macchinari pericolosi; l'uso delle impronte digitali o della topografia della mano a scopi facilitativi; la sottoscrizione di documenti informatici. Pertanto, attraverso il Provvedimento generale e le contestuali Linee guida, il Garante predisponeva un primo quadro unitario nella disciplina giuridica italiana relativa ai sistemi biometrici, individuando misure e accorgimenti di carattere tecnico, organizzativo e procedurale idonee a orientare i titolari dei trattamenti nell'adozione di sistemi biometrici in modo conforme alla disciplina sulla protezione dei dati. In esse venivano inoltre analizzate in modo dettagliato le forme di trattamento svolte da soggetti pubblici o privati per finalità di riconoscimento biometrico, escludendo tuttavia le forme di trattamento rivolte a finalità di sicurezza, giustizia e ricerca scientifica[147]. Nei successivi paragrafi analizzeremo in maggior dettaglio l'evoluzione dell'attività del Garante per la protezione dei dati personali in materia di biometria.

2. L'adeguamento interno alla normativa europea in Italia dall'adozione del d.lgs. n. 101/2018 al "d.l. Capienze"

La disciplina sulla privacy e la tutela dei dati personali è una prerogativa del diritto europeo, le cui disposizioni devono essere recepite dai singoli stati membri all'interno dei loro ordinamenti. Nel

[146] Le misure di carattere generale applicabili ai trattamenti di dati biometrici sono descritte al punto 8 delle LG Biometria.
[147] M. Soffientini, *Privacy, protezione trattamento dei dati*, cit., p. 277.

nostro paese ciò è avvenuto con il recepimento della direttiva 95/46/CE e il successivo riordino della materia attraverso il Codice privacy nel 2003, ma per quanto concerne l'affermazione di una disciplina specifica relativa ai sistemi di riconoscimento biometrico, fino all'approvazione del Regolamento (UE) 679/2016 l'unica attività rilevante è stata quella del Garante per la privacy con l'emanazione nel 2014 del Provvedimento generale e delle contestuali Linee guida. Dopo l'approvazione del GDPR nel 2016, per garantire la sua attuazione entro i termini prestabiliti, il legislatore italiano ha adottato il decreto legislativo n. 101/2018 di adeguamento del Codice privacy alle disposizioni del nuovo regolamento europeo[148].

Rispetto al Codice italiano, il nuovo regolamento europeo introduce un approccio alla tutela dei dati personali diametralmente diverso, fondato su un principio di responsabilizzazione (c.d. accountability)[149] degli operatori della rete, stabilendo per il titolare del trattamento l'obbligo di predisporre un insieme di misure adeguate per implementare i principi del GDPR[150]. Le misure previste anteriormente dal Codice privacy per il titolare del trattamento risultavano, invece, piuttosto scarne e limitate, per questo in sede di adeguamento i legislatori italiani hanno constatato che la maggior parte delle previsioni disposte dal d.lgs. n. 196/2003 fossero da abrogare, in quanto incompatibili con le nuove previsioni del GDPR[151].

Conseguentemente, il Garante ha definito "per novellazione"[152] la tecnica di adeguamento adoperata durante i lavori parlamentari per il d.lgs. n. 101/2018, in quanto essendo stato emanato in tempi recenti il Codice italiano conteneva una disciplina collimante in più punti con la disciplina del GDPR, accostando spesso misure molto simili ma non perfettamente coincidenti e richiedendo pertanto un delicato lavoro di riassetto normativo. Le modifiche introdotte dal d.lgs. n. 101/2018 al d.lgs. n. 196/2003 hanno determinato l'emersione di un "nuovo Codice privacy" a tutti gli effetti. Di seguito ripercorreremo brevemente la disciplina generale per il trattamento dei dati sensibili (all'interno dei quali i dati biometrici risultano ricompresi) introdotta dal d.lgs. n. 101/2018 rispetto alle innovazioni apportate dal GDPR, mentre successivamente ci concentreremo in dettaglio sulle misure specifiche in materia di dati biometrici. Il primo aspetto da considerare riguarda l'art. 2-ter Codice privacy, il quale introduce nel nostro ordinamento le basi giuridiche previste dalle lett. c) e e) dell'art. 6, par. 1

[148] Decreto legislativo 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), G.U. Serie Generale n. 205 del 4 settembre 2018.

[149] J. Lindqvist, *New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a World of the Internet of Things?*, in *International Journal of Law and Information Technology*, 2018, 26, p. 57-58.

[150] R. Zaccaria, A. Valastro, E. Alabanesi, *Diritto dell'informazione e della comunicazione*, decima edizione, Wolters Kluwer, CEDAM, 201.

[151] M. Soffientini, *Privacy, protezione trattamento dei dati*, cit., p. 8.

[152] Garante per la protezione dei dati personali, *Relazione annuale 2018* (doc. web. 9109211), p. 13.

GDPR relativo alle condizioni di liceità del trattamento. Esso, infatti, regola i trattamenti di dati personali necessari per l'adempimento di un obbligo giuridico (lett. c) e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (lett. e), i quali richiedono necessariamente la presenza di ulteriori disposizioni nazionali che specifichino la natura degli obblighi giuridici o degli interessi pubblici coinvolti[153]. Sulla base del comma 1 del presente articolo, questa base giuridica può essere disposta unicamente da una norma di legge o, nei casi previsti dalla legge, di regolamento. Queste disposizioni integrative determinate dal diritto nazionale possono essere definite come "presupposte" ai sensi dell'art. 6, par. 2 GDPR[154], che riconosce agli Stati membri un margine di intervento per quanto concerne le forme di diritto nazionale presupposte, le quali devono essere individuate selezionando le fonti richiamabili nel nostro ordinamento.

Di fatto, agli Stati membri è concesso solo l'adozione di misure più specifiche in riferimento a queste basi giuridiche (lett. c e lett e), per determinare forme di trattamento più adeguate alle esigenze dei singoli ordinamenti nazionali. L'art. 6, par. 2 non è l'unica disposizione del GDPR che riconosce una particolare autonomia ai diritti nazionali nella possibilità di ampliare la disciplina europea, infatti anche l'art. 9, par. 4 GDPR adotta un orientamento simile per la regolazione delle categorie particolari di dati. Di fatto, in relazione alla disciplina generale per i dati personali dell'art 2-ter Codice privacy l'intervento del legislatore italiano, rispetto al legislatore europeo, in materia di dati biometrici, si determina all'interno dell'art. 2-sexies, riguardante il trattamento di categorie particolari di dati personali necessario per motivi d'interesse pubblico rilevante[155].

All'interno della nuova disciplina del GDPR i dati biometrici, sulla base dell'art. 9, par. 1, sono classificati come dati sensibili per i quali vige un divieto generale di trattamento per scopi di identificazione, mentre il paragrafo 4 del medesimo articolo ha reso possibile per ogni Stato membro introdurre ulteriori condizioni, o limitazioni, con riguardo al trattamento di dati genetici, biometrici o relativi alla salute. Pertanto, la disciplina di recepimento italiana ha adottato le disposizioni europee per i dati biometrici, stabilendo al contempo una disciplina specifica per i dati sensibili in riferimento a motivi di interesse pubblico rilevante. Ai sensi dell'art. 2-sexies Codice privacy, comma 1, i trattamenti di dati sensibili regolati dall'art. 9, par. 1 GDPR, necessari per motivi di interesse pubblico rilevante (art. 9, par. 2, lett. g), sono ammessi solo qualora siano previsti dal diritto dell'Unione

[153] L. Bolognini, E. Pelino, *Codice privacy: tutte le novità del d.lgs. 101/2018: in vigore dal 19 settembre 2018,* Il Civilista, Giuffrè Francis Lefebvre, 2018, p.14.

[154] Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.

[155] E. Lucchini Guastalla, *Privacy e Data Protection: principi* generali, in V. Franceschelli, E. Tosi (a cura di), *Privacy Digitale, Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Diritto delle nuove tecnologie, Giuffrè Francis Lefebvre, 2019, p. 69.

europea ovvero, nell'ordinamento interno, da disposizioni di legge o nei casi previsti dalla legge, da regolamenti, che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi del soggetto interessato. Il primo comma, pertanto, stabilisce le misure relative ai dati sensibili a cui deve adeguarsi il diritto nazionale presupposto dall'art. 9, par. 2, lett g) GDPR, dando una linea di continuità con l'abrogato art. 20 Codice privacy, relativo ai principi applicabili ai dati sensibili[156]. Per la regolazione di queste forme di trattamento si determina pertanto una riserva di legge relativa, in quanto si attribuisce alla legge la disciplina dei principi della materia e a fonti secondarie la loro implementazione e la predisposizione della normativa integrativa, ai sensi degli artt. 23 e 97 Cost. Il secondo comma del medesimo articolo invece stabilisce, fermo restando quando sancito dal primo comma, un elenco di ipotesi specifiche nelle quali sussiste per disposizioni di legge, o nei casi previsti dalla legge, l'interesse pubblico rilevante, applicabili sia a soggetti pubblici che privati. Rispetto alla stesura originale del Codice, le innovazioni introdotte dal d.lgs. n. 101/2018 riguardano prevalentemente l'estensione di queste previsioni a soggetti privati e l'aggiunta di ulteriori ipotesi quali i rapporti tra soggetti pubblici ed enti appartenenti al terzo settore.

Le ipotesi elencate all'interno del suddetto comma non riducono l'effetto delle previsioni introdotte nel primo comma, in quanto l'interesse pubblico deve essere riconosciuto in ogni caso *ex lege* sulla base del diritto nazionale. Tuttavia, nonostante il trattamento sia individuato attraverso le previsioni di un'apposita disposizione normativa, il secondo comma dell'art. 2-sexies individua in un elenco ingessato e poco esaustivo tutte le forme di trattamento che possano essere effettuate per motivi di interesse pubblico rilevante, prima divise all'interno di diverse disposizioni del Codice[157].

Il limite principale di questa nuova previsione è dovuto, quindi, al fatto che il nuovo art. 2-sexies intervenga limitando eccessivamente la materia rispetto alla flessibilità introdotta invece dall'art. 9, par. 2 GDPR, specialmente per quanto concerne il settore privato, in quanto il diritto nazionale presupposto si riduce in questo caso in modo specifico ai casi regolati da norme di legge o nei casi previsti per legge, di regolamento. Restano escluse forme di diritto nazionale presupposte quali atti amministrativi generali, linee guida, circolari e forme di soft law, mentre la definizione di queste forme di trattamento resta ancorata a iter legislativi che spesso richiedono tempi molto ampi, rispetto alla tempestività delle evoluzioni in questo settore. Da ultimo il terzo comma dell'art. 2-sexies, dedicato in modo specifico al trattamento di dati biometrici, genetici e sanitari, stabilisce per questi ultimi l'applicazione delle previsioni sancite dall'art. 2-septies Codice privacy, che ne regola la disciplina in modo specifico. L'art. 2-septies rappresenta una delle maggiori innovazioni introdotte

[156] L. Bolognini, E. Pelino, *Codice privacy: tutte le novità del d.lgs. 101/2018: in vigore dal 19 settembre 2018,* cit., p.17-18.

[157] L. Bolognini, E. Pelino (a cura di), *Codice della Disciplina Privacy*, Giuffrè Francis Lefebvre, 2019, p.117-119.

dal d.lgs. n. 101/2018 e costituisce il cardine della disciplina italiana in materia di dati biometrici[158]. Esso regola la disciplina delle misure di garanzia dei dati genetici, biometrici e relativi alla salute, in aggiunta alle previsioni già stabilite dall'art. 2-sexies. Al primo comma, in attuazione del par. 4 dell'art. 9 GDPR che prevede per ogni Stato membro la possibilità di introdurre ulteriori condizioni o limitazioni in riferimento alla disciplina di queste categorie di dati sensibili, si stabilisce che i dati genetici, biometrici e relativi alla salute possano essere oggetto di trattamento solo in presenza di una delle condizioni elencate al par. 2 art. 9 GDPR e se conformi alle misure di garanzia disposte dal Garante[159]. Le misure di garanzia sono autorizzazioni generali al trattamento dei dati in casi specifici[160], adottate dal Garante per la privacy, che ai sensi del comma 2 dell'art. 2-speties devono essere adottate con cadenza biennale e tenendo conto:

a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;
b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;
c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

Ai sensi del terzo comma del medesimo articolo, inoltre, lo schema del provvedimento che stabilisce le misure di garanzia deve essere sottoposto a un periodo di consultazione pubblica per un periodo di almeno sessanta giorni. Le misure di garanzia sono adottate in relazione alle categorie di dati personali specificate all'interno del primo comma dell'art. 2-septies e in riferimento alle specifiche finalità del trattamento, possono individuare ulteriori condizioni sulla base delle quali il trattamento di queste categorie particolari di dati è consentito[161]. In particolare, esse individuano le misure di sicurezza, le misure di minimizzazione dei dati[162], le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché altre possibili misure necessarie per tutelare i diritti degli interessati. Ad oggi, il Garante italiano non ha ancora adottato le misure di garanzia relative al trattamento dei dati biometrici ai sensi dell'art. 2-septies e al tempo in cui si scrive tali misure risultano ancora in corso di elaborazione. L'avvio dei lavori per la loro adozione è stato predisposto fra gli interventi programmatici prioritari stabiliti all'interno della Relazione annuale del

[158] L. Bolognini, E. Pelino, *Codice privacy: tutte le novità del d.lgs. 101/2018: in vigore dal 19 settembre 2018,* cit., p. 29.
[159] L. Bolognini, E. Pelino (a cura di), *Codice della Disciplina Privacy,* cit., p.114-115.
[160] A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici,* cit., p. 126-127.
[161] Vedere Art. 2-septies, comma 5 Codice Privacy.
[162] Il principio di minimizzazione dei dati è disciplinato dall'art. 5 GDPR, il quale prevede che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati: Pertanto non è consentito trattare dati non necessari rispetto alle finalità per le quali sono raccolti.

2019 del Garante[163]. Nonostante l'attesa per l'adozione di queste misure, la disciplina transitoria dell'art. 22, comma 11 del d.lgs. n. 101/2018 stabilisce che le disposizioni del Codice relative al trattamento di dati genetici, biometrici o relativi alla salute (ossia anche quelle abrogate dallo stesso decreto), continuino a trovare applicazione, in quanto compatibili con il GDPR, fino all'adozione delle corrispondenti misure di garanzia di cui all'articolo 2-septies Codice privacy introdotto dal presente decreto[164]. La corretta individuazione della suddetta normativa ancora applicabile in forma transitoria è ancora sede di discussione in dottrina, specialmente per quanto concerne la disciplina secondaria derivata da queste misure ora abrogate nel decreto di adeguamento[165].

Questa disposizione sembra concedere la possibilità continuare ad applicare al trattamento dei dati biometrici le procedure delle Linee guida sulla biometria del 2014, conformandone le disposizioni alla nuova disciplina del GDPR. Tuttavia, l'esercizio di questa valutazione caso per caso della compatibilità delle vecchie disposizioni con la nuova disciplina del GDPR rischia di generare una forte confusione nei titolari del trattamento di queste categorie particolari di dati, per questo è auspicabile un urgente intervento da parte del Garante per risolvere questa condizione di incertezza normativa.Da ultimo, l'art. 2-speties, comma 7 Codice privacy consente, nel rispetto dei principi in materia di tutela dei dati personali e con riferimento alle previsioni dell'art. 32 del GDPR sull'adozione di adeguate misure di sicurezza per il trattamento, l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte di soggetti autorizzati nel rispetto delle misure di garanzia di cui al presente articolo. Una volta adottato il provvedimento del Garante sulle misure di garanzia, le previsioni in materia di sicurezza del trattamento di questi dati sensibili dovranno certamente essere adeguate alle disposizioni in esso contenute.

Il comma 7 dell'art 2-septies costituisce, di fatto, un'innovazione in linea con gli sviluppi presenti essendo ormai i sistemi biometrici di indubbia utilità come sistemi di controllo e autenticazione all'interno di contesti aziendali sempre più tecnologici e informatizzati, sebbene sia in ogni caso escluso il loro utilizzo nei casi di accesso logico o fisico in ambienti privi di dati[166]. Il trattamento di dati biometrici viene pertanto concesso anche per le rilevazioni degli accessi fisici a luoghi di conservazione di dati genetici e campioni biologici[167]. Successivamente all'adozione del d.lgs. n. 101/2018, vi è un'ulteriore innovazione legislativa in materia di biometria della quale tener conto

[163] Garante per la protezione dei dati personali, *Relazione annuale del 2019* (doc. web. 9428236).
[164] Altre disposizioni transitorie e finali, Art. 22, comma 11, d.lgs. n. 101/2018.
[165] L. Bolognini, E. Pelino, *Codice privacy: tutte le novità del d.lgs. 101/2018: in vigore dal 19 settembre 2018,* cit. p. 30-37.
[166] In realtà come vedremo l'utilizzo di dati biometrici con riguardo alle procedure di accesso fisico e logico da parte di soggetti autorizzati in ambienti privi di dati è consentito in casi che richiedono controlli stringenti sulla base della presenza di alti rischi, che richiedono specifici livelli di sicurezza.
[167] A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici,* cit., p. 120.

nella presente analisi. In particolare, l'art. 9 del decreto legge 8 ottobre 2021 n. 139[168], noto anche come "DL Capienze", ha disposto una piccola riforma di alcune previsioni del Codice Privacy, concedendo alle pubbliche amministrazioni la possibilità di trattare e diffondere dati personali[169]. Questi interventi normativi, dapprima molto criticati in dottrina, sono stati parzialmente corretti attraverso la legge di conversione n. 205/2021[170], che ha inserito un'ulteriore previsione in materia di sistemi di riconoscimento biometrici.

Questa liberalizzazione del trattamento di dati da parte di enti pubblici, attraverso la legge di conversione, si esplica in una modifica al testo dell'art. 2-ter Codice privacy. Se, infatti, dapprima il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri era concesso solo ove previsto da una norma di legge o, nei casi previsti dalla legge, di regolamento, ad oggi queste forme di trattamento possono essere regolate anche da atti amministrativi generali emanati da pubbliche amministrazioni, certamente in modo conforme a quanto disposto dal GDPR e dal Codice privacy[171].

Lo stesso intervento modificativo disposto dall'art. 9, lett a) l. n. 205/2021 per l'art. 2-ter, comma 1 Codice privacy, viene disposto alla lettera b) del medesimo articolo per l'art. 2-sexies, comma 1 Codice privacy. Pertanto, anche per quanto concerne il trattamento di dati particolari per motivi di interesse pubblico rilevante, il loro trattamento viene ammesso anche qualora sia previsto da atti amministrativi generali, pur in assenza di una norma di legge. Attraverso questa modifica dell'art. 2-sexies si determina un forte ampliamento nella categoria di soggetti pubblici coinvolti nella regolazione diretta di queste forme particolari di trattamento, rischiando di introdurre forti differenze fra enti pubblici con ruoli e compiti diversi[172]. Tuttavia, anche nel caso di atti amministrativi generali resta in vigore il principio di necessità e l'obbligo di specificare in dettaglio il trattamento e le misure adottate per implementare la tutela dei diritti fondamentali degli interessati, ai sensi dell'art. 9 GDPR. Inoltre, restano sempre valide le previsioni al comma 8 dell'art. 2-septies Codice privacy per cui è tassativamente vietata la diffusione di dati genetici, biometrici o relativi alla salute. Attraverso la

[168] Decreto legge 8 ottobre 2021, n.139 – Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali, G.U. Serie Generale n. 241 del 8/10/2021.

[169] M. Martotana, *Decreto Capienze: come è intervenuto sul Codice della Privacy*, in *Altalex*, 13 ottobre 2021. https://www.altalex.com/documents/news/2021/10/13/decreto-capienze-come-intervenuto-codice-privacy

[170] Legge 3 dicembre 2021, n. 205, Conversione in legge, con modificazioni, del decreto legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali, G. U. Serie Generale n. 291 del 7/12/2021.

[171] A. Cataleta, *DL Capienze, meno privacy per tutti: novità e rischi*, in *Agenda Digitale*, 8 ottobre 2021. https://www.agendadigitale.eu/sicurezza/privacy/dl-capienze-meno-privacy-per-tutti-novita-e-rischi/

[172] M. Bassini, *DL Capienze, perché indebolire la privacy? I dubbi di forma e di sostanza*, in *Agenda* Digitale, 9 novembre 2021. https://www.agendadigitale.eu/sicurezza/privacy/dl-capienze-perche-indebolire-la-privacy-i-dubbi-di-forma-e-di-sostanza/

legge di conversione n. 205/2021 è stata adottata su proposta del Senatore Sensi[173] una moratoria sull'utilizzo di sistemi di videosorveglianza basati sul riconoscimento biometrico all'interno di spazi pubblici, ispirata alla risoluzione adottata dal Parlamento europeo lo scorso 6 ottobre 2021. La moratoria prevista fino al 31 dicembre 2023 e rivolta sia a soggetti pubblici che privati, ha ad oggetto il divieto di utilizzo di sistemi di sorveglianza basati su sistemi di riconoscimento biometrico all'interno di spazi pubblici. Vi è però un'eccezione, in quanto se questi trattamenti rientrano all'interno di finalità di prevenzione e contrasto al crimine previo parere favorevole del Garante è possibile effettuarli. Inoltre, suddetto parere non risulta necessario nel caso in cui il trattamento sia svolto da un'autorità giudiziaria o da un pubblico ministero. Di fatto, l'adozione di questa previsione in realtà fa fare un passo indietro al nostro paese nella predisposizione di garanzie per i cittadini rispetto al trattamento di questi dati sensibili da parte di autorità di polizia giudiziaria e pubblici ministeri[174]. Come vedremo nei prossimi paragrafi, prima dell'adozione di questa moratoria, ai sensi del d.lgs. 18 maggio 2018, n. 51 le autorità giudiziarie e di polizia erano tenute ad ottenere un parere favorevole da parte del Garante privacy prima di poter intervenire: una misura di controllo preventivo che ora non si rende più necessaria in questo tipo di interventi[175]. La messa al bando di questi sistemi di riconoscimento biometrico all'interno di spazi pubblici viene rivendicata anche all'interno del movimento "Reclaim Your Face"[176], iniziativa dei cittadini europei promossa per richiedere alla Commissione europea limitazioni stringenti dell'uso di sistemi di sorveglianza di massa da parte di pubblici poteri. All'interno di questa campagna europea collabora anche il nostro paese attraverso il centro Hermes[177], per la trasparenza e i diritti umani digitali.

3. Gli interventi del Garante per la protezione dei dati personali in materia di biometria dopo l'adozione del GDPR

Abbiamo già contestualizzato come il nostro Garante privacy abbia svolto nel tempo un ruolo essenziale nel colmare il vuoto normativo in materia di dati biometrici, promuovendo l'adozione nel 2014 del Provvedimento generale e delle Linee guida in materia di biometria, svolgendo spesso un

[173] Per approfondire vedere il Dossier n° 441 – Progetti di legge, 25 maggio 2021, Documentazione per l'esame di progetti di legge – Sospensione dell'istallazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici in luoghi pubblici o aperti al pubblico A. C. 3009. http://documenti.camera.it/leg18/dossier/pdf/AC0497.pdf?_1621957521595

[174] E. Pelino, *Riconoscimento facciale, perché la moratoria non basta: tutti i nodi della norma italiana*, in *Agenda Digitale*, 6 dicembre 2021. https://www.agendadigitale.eu/sicurezza/privacy/riconoscimento-facciale-perche-la-moratoria-non-basta-tutti-i-nodi-della-norma-italiana/

[175] L. Carrer, *La moratoria sul riconoscimento facciale approvata in Italia ci ricorda perché dobbiamo chiedere un divieto*, articolo pubblicato sul sito del centro di ricerca Hermes, 2 dicembre 2021. *https://www.hermescenter.org/italia-moratoria-riconoscimento-facciale-ban-divieto/*

[176] Sito ufficiale della campagna Reclaim Your Face: https://reclaimyourface.eu

[177] Sito ufficiale del centro di ricerca Hermes: https://www.hermescenter.org/it/campagne-2/eci-riprenditi-la-faccia/

vero e proprio ruolo di supplenza nei confronti del legislatore italiano. Inoltre, quando il nostro Parlamento è stato chiamato ad intervenire disciplinando in modo puntuale i dati biometrici, è stato attribuito al Garante il ruolo tecnico di predisposizione delle misure di garanzia per il loro trattamento. Nonostante ciò il ruolo ricoperto dalla nostra Autorità indipendente è stato non solo quello di orientare, supervisionare e integrare l'attività del legislatore, ma anche quello di svolgere una vera e propria azione di coordinamento, direzione e controllo sull'applicazione di questa disciplina da parte di enti pubblici e privati[178]. Successivamente all'adozione del GDPR e al suo recepimento nel nostro ordimento, il Garante ha continuato a ricoprire un ruolo di primaria importanza nel garantire la sua corretta implementazione, supervisionando l'attività di soggetti pubblici e privati.

Già nel 2017, infatti, il Garante privacy aveva concesso il via libera, previa verifica preliminare, a un sistema informatico in grado di verificare via web l'identità degli avvocati iscritti a corsi di formazione professionali erogati online, per evitare che gli iscritti simulassero la loro partecipazione per ottenere in modo illegittimo i loro crediti formativi[179]. Nel provvedimento in questione[180], il Garante ribadiva la necessità di effettuare una distinzione fra la rilevazione del singolo carattere biometrico (dato del volto, impronta digitale) e la fonte alla base dello stesso (una fotografia, il dito di un soggetto), in quanto può ritenersi dato biometrico solo il dato personale che una volta raccolto sia sottoposto a forme di rilevamento automatizzate, attraverso strumenti volti a identificare in modo univoco una persona fisica. Solo in tal caso lo si può ritenere a tutti gli effetti un trattamento di dati biometrici ai sensi del GDPR. L'obiettivo del provvedimento era quello di stabilire come i dati acquisiti per il riconoscimento via webcam non fossero dati biometrici in quanto non processati attraverso sistemi automatizzati, anche se in esso tuttavia il Garante finiva per ribadire un assunto generale secondo il quale per far sì che si parli di trattamento di dati biometrici è essenziale che la verifica dell'identità sia effettuata in forma automatizzata, attraverso appositi software. La semplice pubblicazione sui social media di una nostra foto o di una registrazione video, di fatto non configura di per sé un trattamento di dati biometrici. Certamente, questi file online possono essere processati attraverso sistemi di rilevazione biometrica per disporne un trattamento, ma ciò può avvenire solo in presenza di una legittima base giuridica, ai sensi degli artt. 6 e 9 GDPR, di un'apposita informativa e in modo congruo e proporzionato rispetto alle finalità perseguite.

Nell'anno successivo, attraverso un ulteriore provvedimento volto a fornire indicazioni preliminari per favorire la corretta applicazione del GDPR, il Garante ha stabilito, nei casi di trattamento di dati personali tramite strumenti automatizzati fondati sulla base giuridica del legittimo interesse, che esso

[178] M. Soffientini, *Privacy, protezione trattamento dei dati*, cit., p. 512-514.

[179] Garante per la protezione dei dati personali, *Regolamento privacy, come scegliere il responsabile protezione dati (RPD) – Ced Vinianale, definite procedure privacy*, Newsletter n. 432 del 15 settembre 2017.

[180] Garante per la protezione dei dati personali, *Verifica preliminare, riconoscimento via webcam dei partecipanti a corsi di formazione in diretta streaming*, 26 luglio 2017 (doc. web. 6826368).

non possa configurarsi in relazione ai dati biometrici. Essi, di fatto, non possono essere trattati sulla base del legittimo interesse del titolare in quanto, come sottolineato dall'autorità, "nel trattare dati personali sulla base del legittimo interesse proprio o di terzi, è necessario tenere in debita considerazione tra gli altri (…) che il trattamento non riguardi le categorie particolari di dati personali enumerate all´art. 9, par. 1, del Regolamento (tra i quali sono inclusi i dati biometrici che, rispetto al regime previgente stabilito dal Codice, vengono, così, sottratti alla possibilità di essere trattati in base al presupposto del legittimo interesse), né i dati relativi a condanne penali e reati di cui all´art. 10 del Regolamento"[181]. Questo provvedimento, come vedremo, ha inciso notevolmente sulla disciplina sul trattamento dei dati biometrici nei rapporti di lavoro, sulla quale il Garante è intervenuto in più occasioni nel tempo senza mai individuare un'univoca base giuridica per queste forme di trattamento. Nei successivi paragrafi saranno analizzate in dettaglio le basi giuridiche delle varie tipologie di trattamento in materia di biometria individuate all'interno del nostro ordinamento, compreso il trattamento effettuato nei rapporti di lavoro, il trattamento da parte di pubbliche amministrazioni e da autorità di pubblica sicurezza. In questa sede, preliminarmente, ci interessa individuare alcuni casi di particolare rilievo che leghino l'attività del Garante privacy all'evoluzione della disciplina italiana sulla biometria. A tal proposito in ambito lavorativo, L'EDPB nelle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video aveva già espresso l'orientamento per cui dato il forte squilibrio di potere fra datore e dipendente, nella maggior parte dei casi i datori di lavoro non dovrebbero invocare il consenso nel trattare dati personali in quanto è difficile stabilire se quest'ultimo sia concesso liberamente[182].

Anche se l'utilizzo di dati biometrici in ambito lavorativo è stato autorizzato in alcuni casi in passato dal Garante privacy, specialmente nel contesto di verifica degli accessi ad aree di particolare criticità per la sicurezza dei lavoratori, tutela di beni, processi produttivi pericolosi o documenti soggetti a segretezza, recentemente la nostra Autorità ha adottato provvedimenti più restrittivi sull'impiego di questi sistemi di riconoscimento. Nello specifico recentemente il nostro Garante ha espresso numerosi pareri[183] in merito all'adozione da parte delle pubbliche amministrazioni di sistemi di rilevazione

[181] Garante per la protezione dei dati personali, *Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679*, Provvedimento del 22 febbraio 2018 (doc. web. 8080493).

[182] European Data Protection Board, *Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, Versione 2.0, adottate il 29 gennaio 2020, p. 15, punto 47.

[183] Garante per la protezione dei dati personali, *Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56 recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"*, 19 Settembre 2019 (doc. web.9147290); ID., *Audizione del Presidente dell'Autorità Garante per la protezione dei dati personali nell'ambito dell'esame del disegno di legge C. 1433 recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*, 6 febbraio 2019 (doc. web. 9080870); ID., *Audizione informale di Antonello Soro, Presidente del Garante per la protezione dei dati personali, sul disegno di legge n. 920, recante interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo*, 27 novembre 2018 (doc. web. 9064421); ID., *Parere su uno schema di disegno di legge recante "Interventi per la*

biometrica delle presenze dei loro dipendenti come misura di contrasto all'assenteismo. Nel concreto, la posizione del Garante è stata espressa in relazione a quanto disposto dall'art. 2 della legge 19 giugno 2019, n. 56[184], recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo". Suddetto articolo prevede per le pubbliche amministrazioni la possibilità di effettuare un trattamento di dati biometrici per verificare l'osservanza dell'orario di lavoro da parte del dipendente pubblico, introducendo "sistemi di identificazione biometrica e di videosorveglianza in sostituzione dei diversi sistemi di rilevazione automatica attualmente in uso"[185], conformemente al diritto europeo e al diritto nazionale.

Il trattamento di dati biometrici svolto per finalità di rilevazione delle presenze dei dipendenti pubblici è stato affrontato anche all'interno della già citata Relazione annuale del 2019[186]. In essa il Garante riconosce, a partire dalla disciplina dell'art. 9 GDPR, come il trattamento di dati biometrici (di norma vietato), sia consentito in ambito lavorativo (sia pubblico che privato) solo quando "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro [...], nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" ai sensi dell'art. 9, par. 2, lett b) GDPR. Queste disposizioni tradotte all'interno del nostro ordinamento, implicano anche una conformità di queste previsioni alle misure di garanzia disposte dal Garante ai sensi dell'art. 2-septies Codice privacy, ancora in corso di adozione. Inoltre, la disciplina posta dall'art. 2 l. n. 56/2019 risulta operativamente vincolata all'adozione di un D.P.C.M., su proposta del Ministero della funzione pubblica, previa intesa con la conferenza Stato-Regioni e il parere del Garante privacy, che ancora non è stato emanato. Pertanto, questa incompletezza dell'iter normativo della legge n. 56/2019 determina attualmente l'assenza di una valida base giuridica per queste tipologie di trattamento, non essendovi le previsioni attuative che avrebbero dovuto specificare le caratteristiche e modalità del trattamento e le garanzie a tutela degli interessati.

Un caso di attualità nel quale si è reso esplicito questo orientamento da parte del Garante privacy, riguarda un'ordinanza di ingiunzione[187] disposta il 14 gennaio 2021 nei confronti di un'Azienda sanitaria provinciale. L'ordinanza ha previsto una sanzione amministrativa di trentamila euro per

concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo, 11 ottobre 2018 (doc. web. 9051774).

[184] Legge 19 giugno 2019, n. 56 – Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo, G.U. Serie Generale n. 145 del 22 giugno 2019.

[185] Vedere in dettaglio art. 2, comma 1 l. n. 56/2019.

[186] Garante per la protezione dei dati, Relazione 2019, vedere il punto 13.12, il trattamento di dati biometrici dei dipendenti pubblici per finalità di rilevazione delle presenze.

[187] Garante per la protezione dei dati personali, *Ordinanza di ingiunzione nei confronti di Azienda sanitaria provinciale di Enna*, 14 gennaio 2021 (doc. web. 9542071).

l'Asp della provincia di Enna, per aver adottato un sistema di rilevazione delle presenze dei suoi dipendenti basato sul trattamento di dati biometrici in assenza di una valida base normativa[188]. Il sistema impiegato dall'azienda sanitaria prevedeva l'acquisizione delle impronte digitali dei suoi dipendenti, le quali venivano in seguito memorizzate in forma crittografata sui loro badge personali, mentre il software impiegato effettuava il riconoscimento del soggetto confrontando il dato rilevato al momento della sua acquisizione con l'impronta rilevata al momento della richiesta di accesso. Dunque, secondo il Garante veniva disposto a tutti gli effetti un trattamento di dati biometrici in forma automatizzata in assenza di una legittima base giuridica (ai sensi degli artt. 9 e 6 GDPR) in quanto, non essendo ancora stato adottato il D.P.C.M. previsto dall'art. 2 l. n. 56/2019, non vi era una disposizione normativa in grado di regolare questa topologia di trattamento, garantendo i principi della disciplina sulla protezione dei dati anche in termini di proporzionalità dell'intervento regolatorio rispetto all'obiettivo perseguito (ai sensi dell'art. 6, par. 3, lett. b) GDPR).

Di fatto, essendo possibile ottenere la medesima finalità di riconoscimento attraverso strumenti meno invasivi, quali password di autenticazione o badge di riconoscimento, veniva messo in questione il principio di necessità e l'uso proporzionato di questi dati sensibili rispetto alla finalità di autenticazione perseguita[189]. Inoltre, nel caso in esame non poteva essere evocato nemmeno il presupposto di liceità del consenso da parte dei dipendenti (a fronte di un'informativa adeguata ai sensi dell'art. 13 GDPR), in quanto essendo il lavoratore soggetto a una condizione di subordinazione rispetto al titolare non poteva applicarsi la previsione al par. 4 dell'art. 7 GDPR (condizioni per il consenso)[190], per disporre se il consenso fosse stato prestato liberamente. Da ultimo, è necessario citare anche una recente ordinanza di ingiunzione adottata dal Garante nei confronti dell'Università Bocconi di Milano il 16 settembre 2021[191]. In questa occasione, ad essere contestata, invece, era l'adozione da parte dell'ateneo di due software della società americana Respondus Inc. per lo svolgimento degli appelli d'esame online, durante le restrizioni per la pandemia da Covid-19.

I due software in questione sono denominati "Lockdown Browser" e "Respondus monitor": il primo è in grado di bloccare lo schermo del computer dello studente impedendogli di uscire dalla pagina d'esame e di visualizzare altri file o accedere al web, mentre la seconda effettua un vero e proprio monitoraggio del comportamento dello studente durante l'esame, segnalando all'esaminatore

[188] Garante per la protezione dei dati personali, *Data breach sanitari, Garante privacy sanziona tre strutture – Lavoro: Garante no all'uso delle impronte digitali dei dipendenti se manca base normativa – Dal Consiglio d'Europa le linee guida sul riconoscimento facciale*, Newsletter del 19 febbraio 2021.

[189] A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici,* cit., p. 125-127.

[190] Ai sensi dell'art. 7, par. 4 GDPR nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

[191] Garante per la protezione dei dati personali, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano*, 16 settembre 2021 (doc. web. 9703988).

eventuali anomalie, come ad esempio se lo studente non rivolge lo sguardo allo schermo, si sposta dal monitor o altre situazioni analoghe. Nello specifico, si definisce "*proctoring*" uno strumento di intelligenza artificiale in grado di controllare il dispositivo di uno studente, sia durante la didattica a distanza nelle scuole superiori, che durante prove d'esame per le università.

Da tempo l'uso di queste tecnologie ha suscitato un vivido dibattito in dottrina in quanto, seppur si siano rivelate risorse utili nei periodi di lockdown, secondo alcuni esperti si tratta di tipologie di software poco trasparenti, a volte persino pericolose per la tutela dei dati personali dei soggetti coinvolti[192]. Attraverso l'ingiunzione il Garante ha disposto dunque una sanzione pecuniaria di duecentomila euro nei confronti dell'Università Bocconi, per aver trattato in modo illegittimo i dati dei suoi studenti. A sollevare la questione dinanzi al Garante è stato lo studente inglese Donat Bolton, durante il 2020, quando l'ateneo ha iniziato ad utilizzare questi software nelle sue sessioni d'esame.

I profili di illeceità del trattamento rilevati dal Garante sono molteplici. Da un lato, nel provvedimento si evidenziava preliminarmente come questi sistemi non potessero essere indebitamente invasivi e comportare forme di monitoraggio dello studente sproporzionate rispetto alle finalità perseguite dal trattamento. Inoltre, si constatava da parte dell'ateneo l'inosservanza degli obblighi fondamentali in termini di trasparenza e rilevazione del consenso dei suoi studenti. L'informativa disposta sul sito dell'Ateneo risultava di fatto parziale e incompleta ai sensi dell'art. 13 GDPR, in quanto in essa non veniva riportato il tempo di conservazione dei dati raccolti e il loro trasferimento all'interno di banche dati statunitensi. Il fatto che i dati fossero trasferiti negli Stati Uniti poneva un'ulteriore questione spinosa in quanto ai sensi della *Sentenza Schrems II*[193], che ha invalidato la decisione di adeguatezza della legge statunitense del *Privacy Shield*, adottata nel 2016 dalla Commissione europea dopo la decadenza dell'accordo *Safe Harbor*[194], la Corte di Giustizia dell'Unione europea ha rilevato la non conformità rispetto alle disposizioni europee dei trattamenti svolti dagli Stati Uniti, ad eccezione che ad essi siano applicate le garanzie ulteriori previste nel GDPR o clausole contrattuali standard (CSS)[195].

[192] Per approfondire cfr. K. Hylton, Y. Levy, L. P. Dringus, *Utilizing webcam-based proctoring to deter misconduct in online exams*, in ELSEVIER, *Computers & Education 92-93*, 2016, 53-63; D. Woldeab, T. Brothen, *Online Proctoring, Test Anxiety and Student Performance*, in *Internazional Journal of E-learning & Distance Education*, Vol. 34, No. 1, 2019; S. Dendir, R. S. Maxwell, *Cheating in online courses: Evidence from online proctoring*, in ELSEVIER, *Computers in Human Behavior Reports*, 2020; C. S. Gonzàlez-Gonzàlez, A. Infante-Moro, J. C. Infante-Moro, *Implementation of E-proctoring in Online Teaching:A Study about Mitivational Factors*, in *Sustainability*, MDPI, 2020.

[193] Sentenza della Corte di Giustizia dell'Unione europea (Grande Sezione) del 16 luglio 2020, *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, adottata il 23 luglio 2020, Causa C-311/18.

[194] M. Mensi, *La sicurezza cibernetica*, in M. Mensi, P. Falletta, *Il diritto del web*, Wolters Kluwer, CEDAM, 2018, p.340-344.

[195] Garante per la protezione personale, *Privacy Shield: le FAQ dell'EDPB sulla sentenza Schrems II. Disponibile la traduzione del Garante in italiano*, comunicato del 29 luglio 2020 (doc. web. 9442415).

Pertanto, alla luce delle innovazioni introdotte dalla Sentenza, il Garante ha evidenziato come il trattamento disposto dall'ateneo non potesse ritenersi conforme ai principi di liceità, trasparenza e correttezza, non essendo disposti tutti gli elementi informativi necessari.
Inoltre, anche in questo caso il consenso prestato dagli studenti non poteva ritenersi una base giuridica sufficiente per l'utilizzo di questi software, in quanto non solo l'informativa sulla base della quale lo studente formulava il suo consenso era incompleta, ma anche perché pure in questo caso lo studente si trovava in una posizione di subordinazione rispetto all'ateneo, rendendo difficile determinare se la sua manifestazione di volontà fosse stata concessa liberamente, ai sensi dell'art. 7, par. 4 GDPR. Anche se nella vicenda in questione l'utilizzo dei software non implicava il diretto riconoscimento dello studente, veniva comunque svolto a tutti gli effetti un trattamento di dati biometrici attraverso la raccolta, l'elaborazione e l'analisi del video prodotto dal software tramite strumenti di intelligenza artificiale. La base giuridica per questo tipo di trattamento risultava dunque incompleta sia ai sensi degli artt. 6 e 9 del GDPR, che ai sensi dell'art. 13 GDPR per l'informativa, che in relazione ai principi di minimizzazione dei dati, di limitazione della loro conservazione e di limitazione delle finalità del trattamento, che devono risultare sempre legittime e proporzionate.

3.1 Intervista al Garante per la protezione dei dati personali

All'interno dei lavori di ricerca per lo sviluppo del presente elaborato si è reso possibile intervistare il Garante per la protezione dei dati personali[196]. Questo colloquio è stato rivolto all'approfondimento di questioni tuttora aperte in materia di biometria, in relazione il ruolo svolto dalla nostra Autorità nella sua definizione. Il suo contributo, riassunto nelle risposte ai quesiti riportati in seguito, si è rivelato indispensabile per determinare gli orientamenti futuri del nostro paese nella regolazione dei sistemi di riconoscimento biometrico.

1) Il Garante per la tutela dei dati personali ha svolto negli anni un ruolo essenziale nel colmare il vuoto normativo in materia di biometria antecedente all'introduzione della disciplina del GDPR, promuovendo per esempio l'adozione nel 2014 del Provvedimento generale e delle contestuali Linee guida in materia di biometria, svolgendo un vero e proprio ruolo di supplenza nei confronti del legislatore.

[196] Attraverso il contributo del dott. G. D'Ippolito, attualmente funzionario presso il Garante per la protezione dei dati personali.

All'interno del quadro normativo europeo, qual è il ruolo che la nostra Autorità indipendente può giocare attualmente nel tracciare i limiti formali e materiali della disciplina sui sistemi di riconoscimento biometrico?

Quando parliamo di dati biometrici parliamo di dati particolarmente preziosi per almeno due motivi. Innanzitutto sono dati "unici": non solo perché diretti a identificare in modo "univoco" l'interessato ma anche perché solo difficilmente possono essere modificati (pensiamo per esempio alle caratteristiche comportamenti di una persona, come la sua andatura) o, in altri casi, sono insuscettibili di modifiche nel corso della vita dell'interessato (pensiamo alle caratteristiche del volto, all'impronta digitale o all'iride di una persona). La biometria si pone quindi come una delle sfide future su cui il Garante e la società tutta è chiamata a porre grande attenzione. Per quanto di competenza del Garante, lo stesso è chiamato in primo luogo a valutare la conformità del trattamento di tali dati al rispetto dei diritti e delle libertà fondamentali dell'uomo, tra cui il corretto trattamento dei dati personali, nonché a valutarne la necessità e proporzionalità con riferimento ai principi di una società democratica.
A tal fine può agire in diverso modo, sia *ex ante* che *ex post*. Nel primo caso può agire tramite linee guida, come da lei ricordato, anche nell'ambito del Comitato europeo per la protezione dei dati, tramite l'individuazione delle misure di garanzia di cui all'art. 2-*septies* del d.lgs. 196/2003 o tramite pareri alle istituzioni. Tra questi possiamo ricordare il parere al Ministero dell'Interno su un sistema di videosorveglianza biometrica in tempo reale (Parere sul sistema Sari Real Time, del 25 marzo 2021, doc. web n. 9575877). Nel secondo caso può intervenire tramite provvedimenti correttivi e sanzionatori, come avvenuto nel caso dei dati biometrici acquisiti in spazi pubblici dal Comune di Como, col provvedimento del 26 febbraio 2020 (doc. web n. 9309458). A prescindere dal ruolo del Garante è però importante sottolineare che la tutela dei dati personali potrà davvero contribuire al benessere delle persone solo se smetterà di essere solo un adempimento normativo per diventare innanzitutto un fattore culturale che deve essere insegnato, spiegato, conosciuto dai singoli cittadini e gli stessi ne devono pretendere la tutela in prima persona, nella vita di tutti i giorni e, laddove necessario, anche tramite segnalazione o reclamo al Garante. In altre parole, la vera differenza non la fa il Garante quanto il numero sempre maggiore di cittadini che, per esempio, di fronte sistemi di videosorveglianza biometrica per fini di pubblica sicurezza, considererà non più accettabile sacrificare ciò che c'è di unico nella sua persona per un'illusoria sensazione di protezione.

2) L'avvio dei lavori per l'adozione da parte del Garante delle misure di garanzia per il trattamento di dati genetici, biometrici e relativi alla salute ai sensi dell'art. 2-septies Codice privacy, è stato inserito fra gli interventi programmatici prioritari stabiliti all'interno della Relazione annuale del 2019, ma ad oggi tali misure risultano ancora in corso di elaborazione.

Come ha influito l'avvento della pandemia sui lavori per la loro adozione? È possibile ad oggi fare ipotesi concrete su quali saranno gli orientamenti futuri del Garante privacy in materia di biometria?

Certamente la pandemia è stata un ostacolo non previsto all'interno di un'attività già di per se complessa nella misura in cui l'adozione di tali misure di garanzia, in settori tanto delicati, presuppongono la valutazione di diversi aspetti al fine di bilanciare le esigenze di tutela con quelle del mercato. Per ora il Garante ha adottato le misure di garanzia con riferimento ai dati relativi alla salute e ci si augura di poter licenziare quanto prima anche quelle per i dati biometrici. Nel frattempo, come previsto dall'art. 22, comma 11, del d.lgs. 101/2018, restano salve le disposizioni previgenti laddove compatibili con il Regolamento.
Per quanto riguarda gli orientamenti futuri sul tema, l'auspicio è che sia innanzitutto il legislatore, nazionale ed europeo, a intervenire sul tema. Penso sia compito prima delle assemblee legislative effettuare le scelte più di principio o di politica del diritto sull'approccio che la società tutta deve avere nei confronti di tecnologie tanto impattanti sui diritti e gli interessi delle persone. In tal senso già abbiamo qualche primo segnale nella direzione di veri e propri divieti quanto meno delle tecnologie più rischiose, come quelle che implicano forme di sorveglianza biometrica.
Se così non fosse, il Garante e le altre autorità di controllo non si sottrarranno dal compito di valutare in concreto tali trattamenti e magari ammettere solo quelli che risultato giustificabili in termini di liceità, necessità e proporzionalità con gli obiettivi perseguiti.

3) Nell'attesa dell'adozione di queste misure, la disciplina transitoria dell'art. 22, comma 11 d.lgs. n. 101/2018 stabilisce che le disposizioni del Codice relative al trattamento di dati genetici, biometrici o relativi alla salute, continuino a trovare applicazione, in quanto compatibili con il GDPR, fino all'adozione delle corrispondenti misure di garanzia di cui all'articolo 2-septies Codice privacy.
Tuttavia, la corretta individuazione della suddetta normativa ancora applicabile in forma transitoria è tuttora sede di discussione in dottrina, specialmente per quanto concerne la

disciplina secondaria derivata da queste misure ora abrogate nel decreto di adeguamento, quali le Linee guida sulla biometria del 2014.

L'esercizio di questa valutazione caso per caso della compatibilità delle vecchie disposizioni con la nuova disciplina del GDPR rischia di generare una forte confusione nei titolari del trattamento di queste categorie particolari di dati. Qual è la posizione del Garante in merito all'individuazione di questa disciplina transitoria? Come possono districarsi i soggetti responsabili del trattamento evitando un'indebita sovrapposizione fra la normativa ancora in vigore e quella da disapplicare?

La preoccupazione dei titolari del trattamento è certamente comprensibile e il Garante farà il possibile per ridurre ogni inutile elemento di incertezza. Nel ricordare che è compito del titolare, in virtù del principio di *accountability*, analizzare il proprio trattamento e verificare innanzitutto il rispetto del quadro normativo primario del Regolamento, si può dire che, dei numerosi provvedimenti e atti adottati dal Garante in materia, tendenzialmente sono ancora attuali tutte quelle prescrizioni di principio che fanno riferimento ad aspetti sostanziali del trattamento, come le valutazioni sui fondamenti di liceità del trattamento, sulla sua necessità e proporzionalità, l'analisi del rischio, l'esame delle circostanze fattuali, le misure di sicurezza, ecc. Diversamente, dovranno ritenersi abrogati tutti quegli aspetti procedurali o che fanno riferimento ad istituti non più esistenti, come la richiesta di verifiche preliminari o altre forme di autorizzazione.

4) Le modifiche al Codice della privacy introdotte dall'art. 9 del d.l. 8 ottobre 2021, n.139 denominato "DL Capienze", oltre a incidere sui poteri del Garante attribuiscono alle pubbliche amministrazioni la possibilità di trattare, comunicare e diffondere dati personali. Questo intervento normativo molto criticato è stato modificato con la legge di conversione n. 205/2021, recante fra le altre misure una parziale moratoria (fino al 31 dicembre 2023) sull'uso di sistemi di riconoscimento biometrico all'interno di spazi pubblici, ispirata alla risoluzione adottata dal Parlamento europeo il 6 ottobre 2021. Sulla base delle nuove disposizioni, inoltre, il trattamento di dati particolari, che prima era concesso per motivi di interesse pubblico rilevante solo nei casi previsti dalla legge, potrà ora essere regolato anche da un atto amministrativo generale, ai sensi dell'art. 9 del DL Capienze.

Qual è la posizione del Garante in merito a queste riforme in materia di tutela dei dati personali?
Essendo attualmente lecito il trattamento di dati particolari per motivi di interesse pubblico disposto da un atto amministrativo generale, si ottiene la liberalizzazione della regolazione di queste forme di trattamento da parte di enti pubblici e società a controllo pubblico. Che impatto avrà questa previsione sul rapporto fra autorità pubbliche e la tutela dei diritti dei privati cittadini?
La moratoria sui sistemi di riconoscimento biometrico all'interno di spazi pubblici, predisposta dal legislatore italiano, segna il primo tassello di quello che sarà il futuro orientamento europeo e del nostro paese nella regolazione di questi sistemi?

Il DL Capienze ha certamente avuto un impatto non secondario sulla normativa nazionale e nel rapporto tra Garante e Pubblica Amministrazione. La posizione dal Garante è stata espressa dal Presidente Stanzione nell'ambito delle audizioni al Senato della Repubblica del 2 novembre 2021 dove ha ricordato che il fine della semplificazione deve essere perseguito senza compromettere la tutela del diritto. Ciò può essere fatto adottando i necessari "correttivi" e aggiustamenti, previsti in fase di conversione del decreto, per consentire al Garante di continuare a svolgere il suo ruolo di autorità di controllo.
Se è vero che le amministrazioni avranno un margine di discrezionalità maggiore nel trattamento dei dati personali, la conseguenza è che il Garante aumenterà il suo scrutinio con riferimento ai principi di cui all'art. 5 del Regolamento. Ciò vuol dire che, con riferimento al trattamento posto in essere dal titolare pubblico, si darà meno peso al fondamento di liceità del trattamento per aumentare il controllo sul rispetto degli altri principi previsti dall'art. 5.
Penso quindi alla minimizzazione, alla limitazione delle finalità e conservazione, alla sicurezza, all'esattezza dei dati e così via. In altre parole, il sindacato sui trattamenti svolti dalla pubblica amministrazione diventa più simile a quello che attualmente il Garante già svolge nei confronti dei trattamenti posti in essere dal titolare privato. Con riferimento alla "moratoria" sugli "impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici", come recita la norma, l'auspicio è proprio questo, che il legislatore nazionale ed europeo perseguano in questa direzione vietando o limitando fortemente il ricorso a tali tecnologie.

Attraverso il presente contributo è stato possibile riaffermare il ruolo primario ricoperto dalla biometria nel determinare le sfide future legate alla disciplina sulla privacy, sulle quali il nostro Garante sarà chiamato a porre un'attenzione sempre maggiore.

Nel tracciare i limiti formali e materiali della disciplina sui sistemi di riconoscimento biometrico, la nostra Autorità può attualmente intervenire sia *ex ante*, attraverso l'adozione di linee guida o tramite pareri alle istituzioni, che *ex post*, attraverso provvedimenti correttivi e sanzionatori. Tuttavia, l'aspetto più saliente rispetto alla regolazione dei sistemi biometrici, è legato al ruolo cruciale che la nostra Autorità dovrà ricoprire nel tutelare il benessere delle persone, educarle e trasformarle in soggetti attivi in grado di giocare un ruolo primario nella regolazione di questi sistemi invasivi, attraverso la predisposizione di segnalazioni e reclami. Solo attraverso una sensibilizzazione attiva dei cittadini, di fatto, sarà possibile determinare cosa la nostra società sia disposta a sacrificare nella tutela della propria riservatezza, per convivere con l'implementazione di questi sistemi.

Se le assemblee legislative giocheranno un ruolo cruciale nella definizione degli orientamenti futuri in materia di biometria, le autorità di controllo, in virtù del loro potere indipendente, potranno continuare a valutare in concreto i singoli trattamenti ammettendo solo quelli che in virtù dei principi sanciti dal GDPR risultino giustificabili in termini di liceità, necessità e proporzionalità, in relazione alle finalità perseguite. Qualsiasi fine semplificatorio, di fatto, come disposto dal DL Capienze dovrà essere sempre perseguito senza compromettere la tutela del diritto. In questo senso, se le innovazioni introdotte dal decreto avranno l'effetto di attribuire un margine di discrezionalità maggiore nel trattamento dei dati personali alle amministrazioni, il Garante non esiterà ad estendere il suo scrutinio con riferimento ai principi dell'art. 5 GDPR, per preservare il suo ruolo di attività di controllo. Pertanto, il sindacato svolto dalla nostra Autorità in relazione ai trattamenti svolti da pubbliche amministrazioni diverrà semplicemente più simile a quello già messo in atto nei confronti di titolari privati. Da ultimo, vi è l'auspicio per cui siano le assemblee legislative a intervenire prioritariamente nella limitazione di forme di trattamento lesive della privacy dei cittadini, quali le forme di sorveglianza biometrica all'interno di spazi pubblici, effettuando le scelte di principio e di politica del diritto per orientare il rapporto fra la nostra società e l'intelligenza artificiale.

4. Il trattamento di dati biometrici nell'ordinamento italiano

Rispetto alla disciplina europea, nel nostro ordinamento esistono misure specifiche per regolare alcune tipologie di trattamento di dati biometrici, che di seguito analizzeremo in dettaglio. Di fatto, dopo aver ricostruito gli albori della disciplina italiana in materia di biometria ed il suo sviluppo attraverso il recepimento della normativa europea e l'attività del Garante privacy, è necessario

focalizzarsi sulla regolazione di queste forme di trattamento all'interno di settori specifici, analizzando anche gli illeciti connessi al loro indebito utilizzo e l'applicazione della valutazione d'impatto sulla protezione dei dati (DPIA).

4.1 Firma grafometrica

La firma grafometrica è classificata come una tipologia di firma elettronica avanzata (FEA), ai sensi dell'art. 1, lett. q-bis del Codice dell'Amministrazione Digitale[197]. Essa consiste in una sorta di versione digitale della firma su carta, in quanto registrando i caratteri biometrici legati alla grafia del soggetto al momento di apposizione della sua firma su supporto digitale, tramite la firma grafometrica si associano a un determinato documento informatico i parametri biometrici rilevati, in modo da condurre ex post delle analisi grafologiche per verificare la validità della sottoscrizione[198]. Le informazioni biometriche acquisite attraverso questa raccolta possono rilevare ulteriori connotati del soggetto quali la velocità di scrittura, la pressione esercitata dalla mano, l'inclinazione, fino a rivelare persino informazioni sensibili concernenti lo stato di salute[199], per questo si tratta di una forma di trattamento che necessita di un elevato livello di protezione.

Questa tecnica biometrica viene utilizzata prevalentemente per la sottoscrizione di documenti informatici attraverso dispositivi elettronici (in genere tablet), come disposto dal CAD per la disciplina della firma elettronica avanzata, introdotta inizialmente dal d.lgs. n. 82/2005 e disciplinata in seguito attraverso disposizioni tecniche dal D.P.C.M. 22 febbraio 2013[200]. Nel nostro ordinamento, la FEA consiste in una semplificazione della firma elettronica qualificata, ma per poter essere adoperata con gli stessi effetti giuridici deve essere in grado di garantire una serie di requisiti specificati all'interno del Titolo V del D.P.C.M. 22 febbraio 2013. L'uso della FEA è stato, inoltre,

---

[197] Codice Amministrazione Digitale (CAD), istituito con il d.lgs. 7 marzo 2005, n. 82, è stato in seguito modificato e integrato prima attraverso il d.lgs. 22 agosto 2016 n. 179 e in seguito con il d.lgs. 13 dicembre 2017 n. 217. Le ultime modifiche alla materia sono state apportate dal d.l. 16 luglio 2020, n. 76 convertito dalla l. 11 settembre 2020, n. 120. Fonte pagina dal sito AgID sul CAD. https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione-digitale

[198] M. Soffientini, *Privacy, protezione e trattamento dei dati*, cit., p. 277.

[199] Le tecnologie biometriche sono strettamente connesse a caratteristiche dell'individuo, che possono rivelare informazioni sensibili a livello genetico o sul suo stato di salute. Ad esempio, la struttura vascolare di una mano può rilevare la presenza di alcune malattie cromosomiche oppure la rilevazione della firma può determinare la presenza di malattie neurologiche. Si legga in proposito l'analisi del Comitato Nazionale per la Bioetica, *L'identificazione del corpo umano: profili bioetici della biometria*, 26 novembre 2010. https://bioetica.governo.it/it/pareri/pareri-e-risposte/l-identificazione-del-corpo-umano-profili-bioetici-della-biometria/

[200] Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*, in G. U. Serie Generale n. 117 del 21 maggio 2013.

disciplinato a livello europeo all'interno del Regolamento (UE) n° 910/2014 (eIDAS)[201] sull'identità digitale, nel quale all'art. 26 si dispone che una firma elettronica avanzata debba soddisfare i seguenti requisiti:

a) essere connessa unicamente al firmatario;
b) essere idonea a identificare il firmatario;
c) essere creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e
d) essere collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Nella disciplina italiana, invece, la firma grafometrica, è stata regolata nello specifico dal Garante privacy all'interno del Provvedimento generale del 12 novembre 2014, n. 513 (al punto 4.4 sulla sottoscrizione di documenti informatici) e nelle contestuali Linee guida in tema di riconoscimento biometrico e firma grafometrica. In particolare, all'interno del punto 5.4 delle Linee guida si dispone come l'utilizzo della firma grafometrica per la sottoscrizione di documenti informatici "non richieda la creazione di una banca dati biometrica, poiché le singole firme grafometriche sono volta per volta acquisite e incorporate, con le opportune protezioni crittografiche, nel documento informatico sottoscritto, eventualmente archiviato in un sistema di gestione documentale"[202].
Da ultimo, la firma grafometrica agevola le pratiche per la conclusione di contratti in forma digitale[203] in quanto non richiede che il soggetto sia titolare di un dispositivo di firma, è semplice da utilizzare poiché imita l'apposizione della propria firma autografa e non può essere replicata da soggetti diversi dal firmatario[204]. Allo stesso modo l'impiego di dati biometrici consente un'identificazione rapida e univoca del titolare della firma, garantendo un elevato livello di sicurezza[205].

[201] F. Buffa, *Firme elettroniche e grafometriche, dalla direttiva CE/1999/93 al Regolamento eIDAS 2014/910/UE, in vigore dall'1.7.2016*, Editore Key, Cedon Book, 2016, p. 25-31.
[202] Garante per la protezione dei dati, *Linee guida in materia di riconoscimento biometrico e firma grafometrica*, punto 5.4, p. 18.
[203] E. Tosi, *Diritto privato delle nuove tecnologie digitali, Riservatezza, contratti, responsabilità tra persona e mercato*, Diritto delle nuove tecnologie, Giuffrè Francis Lefevbre, 2021, p. 423.
[204] M. R. Lenti, *Dati biometrici, firma grafometrica e contratti elettronici. Quali implicazioni per la Cyber Security*, in *LUISS Law Review*, n. 2/2017, p. 115-117.
[205] G. Navone, *Il valore giuridico della firma grafometrica*, in *Osservatorio del diritto civile e commerciale*, Fascicolo 1, 2018, p. 115-119.

4.2 Il trattamento di dati biometrici nei rapporti di lavoro

Il trattamento di dati biometrici nei rapporti di lavoro è stato in parte già affrontato in merito ai pareri espressi dal Garante privacy sul testo di legge 19 giugno 2019, n. 56, sulla rilevazione delle presenze dei dipendenti pubblici come misura di contrasto l'assenteismo, e nell'ordinanza d'ingiunzione disposta nei confronti della Asp di Enna ad inizio 2021. In particolare, il Garante ha stabilito come non sia ammissibile in alcun caso l'adozione da parte del datore di lavoro (sia pubblico che privato) di un sistema di rilevazione delle presenze, fondato sull'utilizzo di dati biometrici dei dipendenti, in assenza di una base giuridica che non può prefigurarsi nemmeno sotto il profilo di liceità del consenso del dipendente. In realtà, il Garante era già intervenuto sulla materia a partire dal 2006, con l'adozione delle Linee sul trattamento di dati personali dei lavoratori privati[206] e delle Linee guida sul trattamento di dati personali dei lavoratori pubblici, adottate nel 2007[207]. Entrambe sono state in seguito rimarcate all'interno del Provvedimento generale prescrittivo in tema di biometria del 2014[208] e dopo che il GDPR ha esteso ai dati biometrici la disciplina sui dati sensibili, il nostro Garante ha disposto alcune ulteriori cautele necessarie per regolare queste forme di trattamento.

Essendo i dati biometrici per loro natura strettamente connessi a caratteristiche dell'individuo che possono rivelare numerose informazioni sensibili (anche a livello genetico o sullo stato di salute), per autorizzarne un trattamento deve sempre disporsi un'istanza di verifica preliminare dinanzi al Garante, ad eccezione di alcuni casi specifici puntualmente individuati che possono beneficiare di una esenzione[209]. Inoltre, devono essere sempre disposte le misure tecniche e gli standard di sicurezza richiesti, nonché il rispetto dei principi di liceità, finalità, necessità e proporzionalità del trattamento[210]. Attualmente risulta difficile individuare una legittima base giuridica all'interno del nostro ordinamento per queste forme di trattamento. Come già analizzato, con il Provvedimento del 22 febbraio 2018, la nostra Autorità ha escluso l'interesse legittimo del titolare come possibile base giuridica, ai sensi dell'art. 6 GDPR. Inoltre, con l'ulteriore esclusione in via generale del presupposto del consenso in ambito lavorativo, ai sensi della lett. a) dell'art. 9, par. 2 GDPR[211], risulta difficile

[206] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati*, deliberazione n. 53 del 23 novembre 2006 (doc. web. 1364939).

[207] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*, deliberazione n. 23 del 14 giugno 2007 (doc. web. 14147809).

[208] M. Soffientini, *Privacy, protezione e trattamento dei dati*, Milano, cit., p. 277

[209] Vedere il punto 4 "Esonero della verifica preliminare di cui all'art. 17 del Codice", del Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.

[210] G. Bellomo, *Biometria e digitalizzazione della pubblica amministrazione*, cit., p. 63-67.

[211] L'art. 9, par. 2. lett. a) GDPR rende ammissibile il trattamento di dati biometrici nei casi in cui l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1.

individuare un altro caso di esenzione ai sensi del par. 2, art. 9 che possa giustificare queste forme di trattamento. È possibile ipotizzare che le misure di garanzia disposte all'art. 2-speties del Codice privacy, ancora in corso di elaborazione da parte del Garante, potranno individuare ulteriori condizioni o limitazioni per disciplinare in modo più puntuale il trattamento di dati biometrici in ambito lavorativo.

4.2.1 L'uso delle impronte digitali del lavoratore per accedere ad aree protette

All'interno del Provvedimento 18 giugno 2015, n. 361[212] il Garante privacy ha ritenuto lecito il trattamento di impronte digitali dei dipendenti di una società operante negli spazi commerciali di alcuni aeroporti. Il soggetto in questione predisponeva il trattamento di dati biometrici con la finalità di controllare l'accesso dei dipendenti ad aree sensibili, dove venivano depositati oggetti di pregio e le casseforti contenenti gli incassi dei negozi. In tal caso però data la natura peculiare del sistema di accesso prescelto, non è stato possibile per il Garante applicare per l'azienda l'esonero dall'obbligo di procedimento di verifica preliminare e, inoltre, sono state disposte ulteriori misure di sicurezza per tutelare maggiormente i dati sensibili dei dipendenti[213]. Pertanto, l'uso delle impronte digitali del lavoratore per effettuare l'accesso ad aree protette viene concesso a fronte di una base giuridica legittima, della presentazione di un'istanza di verifica preliminare dinanzi al Garante e della prescrizione di alcune cautele aggiuntive in materia di sicurezza e protezione dei dati.

4.2.2 Il controllo di accesso fisico ad aree sensibili e macchinari pericolosi

Essendo i dati biometrici indice delle caratteristiche fisiche e comportamentali degli individui, possono vantare un profondo legame con il corpo e l'identità della persona a cui si riferiscono. Per questo generalmente vengono adoperati in materia di sicurezza sul lavoro, ai fini di controllo dell'accesso fisico o logico ad aree sensibili o macchinari pericolosi[214]. In particolare, il Garante ha ritenuto lecito l'utilizzo di questi sistemi di riconoscimento biometrico basati sulla rilevazione dell'impronta o della topografia della mano, solo per finalità di sicurezza, per la protezione patrimoniale e la tutela dell'incolumità delle persone[215]. All'interno del Provvedimento generale prescrittivo in tema di biometria del 2014, al punto 4.2 "Controllo di accesso fisico ad aree "sensibili"

[212] Garante per la protezione dei dati personali, *Trattamenti di dati biometrici dei dipendenti. Verifica preliminare*, 18 giugno 2015 (doc. web. 4173465).
[213] M. Soffientini, *Privacy, protezione e trattamento dei dati*, cit., p. 293.
[214] L. Greco, A. Mantalero, *Industria 4.0, Robotica e Privacy-by-design*, in *Il diritto dell'informazione e dell'Informatica,* Anno XXXIX Fasc. 6, 2018, p. 883-884.
[215] A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici,* cit., p. 128.

dei soggetti addetti e utilizzo di apparati e macchinati pericolosi", il Garante dispone un elenco di alcune prescrizioni a fronte delle quali il titolare viene esonerato dall'obbligo di presentazione dell'istanza di verifica preliminare. Inoltre, al suo interno vengono individuate come "aree sensibili", solo[216]:

- le aree destinate allo svolgimento di attività aventi carattere di particolare segretezza, ovvero prestate da personale selezionato e impiegato in specifiche mansioni che comportano la necessità di trattare informazioni riservate e applicazioni critiche;
- le aree in cui sono conservati oggetti di particolare valore o la cui disponibilità è ristretta a un numero circoscritto di addetti;
- le aree preposte alla realizzazione o al controllo di processi produttivi pericolosi che richiedono un accesso selezionato da parte di personale particolarmente esperto e qualificato;
- l'utilizzo di apparati e macchinari pericolosi, laddove sia richiesta una particolare destrezza onde scongiurare infortuni e danni a cose o persone

Sempre secondo la nostra Autorità, nel caso in questione il presupposto di legittimità alla base del trattamento è dato in ambito pubblico dal perseguimento di finalità istituzionali da parte del titolare, mentre in ambito privato dall'applicazione del principio di bilanciamento degli interessi, volto a favorire la sicurezza del lavoratore[217].

4.2.3 Autenticazione informatica ai fini del controllo di accesso o di identificazione degli utenti

Nei casi in cui il dato biometrico sia impiegato come credenziale di identificazione per fornire l'accesso a banche dati o sistemi informatici protetti, o nei casi in cui sia necessario identificare adeguatamente gli utenti per la tipologia di trattamento effettuata o delle risorse informatiche utilizzate, ad alto contenuto sensibile, il Garante ne ha disposto una disciplina puntuale, sempre all'interno del Provvedimento generale del 12 novembre 2014. Al punto 4.1[218], infatti, si dispone come i titolari del trattamento siano esonerati dalla presentazione di un'istanza di verifica dinanzi al Garante, purché siano rispettate le disposizioni elencate nel presente provvedimento.

[216] Vedere il punto 4.2 "Controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi", del Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.
[217] M. Soffientini, *Privacy, protezione e trattamento dei dati*, cit., p. 304.
[218] Vedere il punto 4.1 "Autenticazione informatica", del Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.

Inoltre, anche in questo caso il presupposto di legittimità del trattamento viene fondato in ambito pubblico sulle finalità istituzionali perseguite e in ambito privato attraverso la messa in atto di un bilanciamento di interessi.

4.3 Immigrazione irregolare e trattamento di dati biometrici da parte di Autorità di pubblica sicurezza

Ai sensi della normativa vigente, sia a livello europeo che italiano, il trattamento di dati biometrici è lecito, ai sensi dell'art. 2-septies, comma 1, Codice privacy e dell'art. 9, par. 2, lett. g) GDPR, per motivi di interesse pubblico rilevante, incluso l'uso di questi dati per finalità di pubblica sicurezza, contrasto alla criminalità e prevenzione del terrorismo. Inoltre, come disposto dalla Convenzione di Dublino[219] e dal Trattato di Prüm[220], queste forme di trattamento possono essere impiegate dagli Stati membri per disporre l'esame di una domanda di asilo e contrastare l'immigrazione irregolare[221].
Allo stato attuale, il nostro paese è uno dei più colpiti a livello europeo dal fenomeno migratorio, per questo una delle implementazioni più significative dei sistemi biometrici in ambito di pubblica sicurezza concerne tipicamente l'identificazione di richiedenti asilo. In particolare, ai sensi dell'art. 2 del Trattato di Prüm si dispone l'adozione di appositi schedari nazionali al fine di perseguire violazioni penali, mentre l'art. 8 e seguenti dispongono le misure concernenti la raccolta di dati biometrici. Per favorire inoltre lo scambio fra diversi stati europei, con il Regolamento 2725/2000/CE[222] è stato ideato l'Eurodac[223], ossia un database biometrico istituito con lo scopo di raccogliere le impronte dei richiedenti asilo e i dati di immigrati irregolari. L'adozione di un unico database biometrico europeo ha lo scopo di prevenire che un richiedente asilo formuli una richiesta di accoglienza all'interno di più Stati membri. La banca dati centrale di Eurodac dispone la raccolta dei dati inviati da ogni stato, confrontandoli con i dati precedentemente raccolti in modo da rilevare o meno la presenza delle impronte inserite nel sistema[224]. Ogni impronta registrata viene classificata collegandola al luogo e alla data della sua rilevazione. Inoltre, ogni paese europeo è dotato di un *focal*

[219] Convenzione sulla determinazione dello Stato competente per l'esame di una domanda di asilo presentata in uno degli Stati membri delle comunità europee - Convenzione di Dublino, Gazzetta ufficiale n. C 254 del 19/08/1997.
[220] Il trattato sottoscritto in Germania il 27 maggio 2005 è stato recepito dal nostro paese con la legge 30 giugno 2009, n. 85 e dispone "l'approfondimento della cooperazione transfrontaliera, in particolare al fine di lottare contro il terrorismo, la criminalità transfrontaliera e la migrazione illegale".
[221] A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici*, cit., p. 128-131.
[222] Regolamento (CE) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione della convenzione di Dublino.
[223] Pagina dedicata all'Eurodac, pagina ufficiale del Dipartimento per le Politiche europee. https://www.politicheeuropee.gov.it/it/comunicazione/euroacronimi/eurodac/
[224] A. Sprokkereef, *Data Protection and the Use of Biometric Data in The EU*, in S. Fischer-Hubner, P. Duquenoy, A. Zuccato, L. Martucci, *The Future of Identity in The Information Society*, IFIP International Federazion for Information Processing, Volume 262, Springer, 2008, p. 281-282.

point nazionale competente per disporre il trattamento di questi dati sensibili. Il Servizio di polizia scientifica con sede a Roma costituisce il *focal point* italiano, mentre la Direzione centrale anticrimine costituisce l'autorità responsabile incaricata di Eurodac.

Dopo l'adozione del Regolamento (UE) n. 603/2013[225], l'istituto dell'Eurodac è stato notevolmente modificato attraverso una riforma che ha cercato di mitigarne l'impatto sulla vita dei soggetti coinvolti e nel rispetto del principio di proporzionalità come rilevato dall'EDPS in una sua pronuncia[226]. In particolare all'interno del regolamento si stabilisce come per effettuare queste forme di trattamento la persona debba sempre risultare informata sia per iscritto, che oralmente, in una lingua che risulti comprensibile al soggetto. Inoltre devono essere garantiti i presupposti di un'informativa di base quali l'identità del responsabile del trattamento, le finalità e i destinatari del trattamento, il diritto di accesso ai propri dati e di richiedere una loro rettifica se incorretti, nonché l'esistenza e la natura di un obbligo di rilevamento delle impronte digitali per fini di sicurezza nazionale. Un caso analogo di trattamento di dati biometrici da parte di Autorità di pubblica sicurezza italiane concerne, invece, il casellario centrale d'identità del Dipartimento della pubblica sicurezza del Ministero dell'Interno. Questo casellario fa parte della Direzione centrale anticrimine della Polizia di stato e consente la raccolta dei rilievi fotosegnaletici effettuati dalle forze dell'ordine.

Questi rilievi contenenti le foto, le informazioni anagrafiche e le rilevazioni dei dati biometrici dei soggetti arrestati, consentono la creazione di un grande database nazionale per la prevenzione del crimine, agevolando notevolmente le operazioni di polizia giudiziaria.Da ultimo, nel nostro paese non esiste attualmente un sistema di regole puntuale volto ad orientare i trattamenti di dati biometrici effettuati da forze dell'ordine, in quanto la loro disciplina viene indirizzata prevalentemente dalle disposizioni europee in materia. È auspicabile anche in questo caso, che l'intervento regolatorio disposto dal Garante privacy, ai sensi dell'art. 2-septies Codice privacy, possa intervenire definendo in modo chiaro il quadro normativo di riferimento alla luce dei principi disposti dal Codice e dal Regolamento. In particolare, è sempre necessario garantire l'osservanza del principio di proporzionalità non eccedendo nell'uso di questi sistemi rispetto ai fini perseguiti. In questo senso come già analizzato, in Italia è attualmente in vigore una moratoria sull'uso di sistemi di

[225] Regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (rifusione).

[226] Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] [.....] (Recast version), 05-09-2012.

videosorveglianza basati sul riconoscimento biometrico all'interno di spazi pubblici, ad accezione che il trattamento sia disposto per finalità di pubblica sicurezza, previo parere favorevole del Garante, o sia disposto da un'autorità giudiziaria o da un pubblico ministero.

4.4 Applicazioni della Data protection impact assesment (DPIA)

La valutazione di impatto sulla protezione dei dati (DPIA) introdotta dall'art. 35 GDPR[227] costituisce un onere necessario, posto a carico del titolare del trattamento per valutare i fattori di rischio connessi al trattamento posto in essere, analizzando le conseguenze del trattamento ed il loro impatto sui diritti e le libertà degli interessati. Tuttavia, prima che il GDPR introducesse la disciplina sulla DPIA, il Garante italiano aveva disposto all'interno del Provvedimento generale in tema di biometria del 2014, che alcune tipologie di trattamento per le finalità perseguite e la loro natura contrassegnata da una soglia di rischio bassa, fossero esonerate dall'obbligo di verifica preliminare disposto all'art. 17 Codice privacy (successivamente abrogato dal d.lgs. n. 101/2018).
Questa misura di semplificazione si era resa necessaria data la forte crescita sul mercato delle tecnologie biometriche, anche se essa risultava strettamente vincolata all'adozione di previsioni e accorgimenti tecnici specifici. Inoltre, dovevano essere sempre rispettati i principi generali di liceità, necessità, proporzionalità e l'obbligo di informativa e di segnalazione preventiva al Garante[228]. Ad oggi, l'esonero dal condurre una valutazione di impatto sulla protezione dei dati, come disposto dall'art. 35 GDPR, per i trattamenti effettuati a scopo di riconoscimento biometrico, risulta ancora subordinata all'adozione di tutte le misure e le disposizioni tecniche individuate all'interno del Provvedimento generale, escluso l'obbligo di notificazione preventiva e salvo che intervengano nuove disposizioni adottate dal Garante.

4.5 Il trattamento illecito di dati biometrici

Nei casi fin qui analizzati abbiamo illustrato la disciplina giuridica dei dati biometrici e le loro forme di trattamento lecite. Tuttavia, spesso la raccolta di questa tipologia di dati avviene anche per scopi illegittimi o non dichiarati. Di fatto essi costituiscono una risorsa informativa molto preziosa che se combinata con altri dati sensibili, ricavati da più banche dati, consente di effettuare delle attività di

[227] Ai sensi dell'art. 35, par. 1 GDPR, quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
[228] [228] M. Soffientini, *Privacy, protezione e trattamento dei dati*, cit., p. 298-299.

profilazione estremamente accurate. Senza la predisposizione di misure preventive di controllo, aziende private e soggetti pubblici agirebbero incontestati nell'elaborazione dei profili fisici e comportamentali dei loro soggetti di riferimento.

Questo bagaglio informativo di fatto costituisce un'arma estremamente pericolosa che non solo pregiudica i diritti e le libertà delle persone, come già discusso, ma può dar luogo a forme di discriminazione, di controllo e di condizionamento illecite[229]. Quando l'acquisizione di queste informazioni avviene per scopi illegittimi, la biometria perde la sua funzione di risorsa primaria per la sicurezza, divenendo uno strumento estremamente pericoloso in grado di condizionare enormemente la vita delle persone. Pertanto di seguito analizzeremo i casi più frequenti di uso illecito di questi sistemi[230]. Uno dei casi più frequenti concerne il furto d'identità digitale. Normalmente l'identità di un soggetto si definisce sulla base di una doppia valenza: da un lato abbiamo l'identità legata alla sfera corporea, che ne determina in termini oggettivi il suo riconoscimento, mentre dall'altro si ha la proiezione della sua personalità nel contesto sociale al quale appartiene, che ne filtra la percezione all'interno della società. Anche all'interno della sfera digitale l'identità di un soggetto assume un duplice rilievo, dato che attraverso di essa è possibile sia disporne l'identificazione attraverso sistemi informatici, che ricostruirne la propria rappresentazione sulla rete digitale.

Le componenti digitali che possono determinare l'identificazione di un soggetto sulla rete si differenziano in password di autenticazione, tessere magnetiche connesse a dispositivi elettronici, oppure come nel nostro caso, in componenti biometriche quali impronte digitali, caratteri del volto, dell'iride o della propria voce. Pertanto, il furto di identità digitale si configura come un'appropriazione illecita da parte di soggetti non autorizzati dei caratteri che consentono l'identificazione di un individuo sul web. Inoltre quando il furto di questi dati avviene in relazione a dati biometrici[231], si configura un livello di rischio ancora maggiore in quanto non è possibile modificare le proprie componenti biologiche come nei casi di password d'accesso o per l'uso di *smartcard*. In genere il furto d'identità avviene per mezzo di azioni di infiltraggio su sistemi informatici o l'adozione di condotte fraudolente quali il *phishing*[232], email che dispongono truffe, la sottrazione di dati effettuata attraverso il furto di documenti. All'interno del nostro ordinamento l'art. 494 del Codice penale dispone il delitto di sostituzione della persona, nel quale è possibile ricondurre anche gli illeciti per furto di identità digitale. In esso si prevede la reclusione fino ad un anno per

[229] T. B. Gillis, J. L. Spiess, *Big Data and Discrimination*, cit., p. 463.
[230] M. R. Lenti, *Dati biometrici, firma grafometrica e contratti elettronici. Quali implicazioni per la Cyber Security*, cit. p. 118-124.
[231] Vedere il punto 7.2 "Furto d'identità biometrica" delle Linee guida in materia di riconoscimento biometrico e firma grafometrica, Allegato A al Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.
[232] Il phishing è una tipologia di truffa effettuata sul web, nella quale un soggetto assumendo un'identità fittizia riesce a ingannare la vittima convincendola a inviargli denaro, condividere dati finanziari o codici di accesso.

chiunque sostituisca illegalmente la propria all'altrui persona, o attribuisca a sé o ad altri un falso nome o un falso stato, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno[233]. Inoltre, la Corte Suprema di Cassazione attraverso una delibera ha specificato come questa tipologia di reato possa configurarsi anche all'interno del contesto digitale della rete[234]. Un reato che può configurarsi in concorso al furto d'identità digitale è il reato di frode informatica, regolato ai sensi dell'art. 640-ter. c.p., che si verifica quando il furto d'identità si rivela strumentale al compimento di ulteriori reati, quali frodi finanziarie o altri illeciti penali.

Invece, un altro illecito sempre connesso alla materia in esame riguarda la falsificazione della firma biometrica. In genere la progettazione dei sistemi biometrici avviene attraverso degli standard di sicurezza tesi a impedire che sia possibile ricavare il campione biometrico dal loro funzionamento, essendo la raccolta dei dati un unico processo irreversibile. Se invece il processo di acquisizione del dato viene separato dalla fase della sua elaborazione è più facile incorrere in riproduzioni illecite dei dati per finalità non autorizzate o all'interno di contesti diversi da quello in cui sono stati legittimamente raccolti. Vi è inoltre in questi casi anche un rischio elevato di falsificazione biometrica[235] essendo possibile determinare artificialmente i dati biometrici di un soggetto a partire dai caratteri biologici esistenti. Dalla manipolazione di questi dati è possibile, infatti, determinare in modo fraudolento i tratti biometrici che dispongono l'identificazione del soggetto. Nel nostro ordinamento le misure preventive per far fronte agli illeciti legati al trattamento dei biometrici, sono state disposte dal Garante privacy all'interno del Provvedimento generale e delle linee guida in materia di riconoscimento biometrico e firma grafometrica del 2014. Tuttavia, è possibile che con l'evoluzione della disciplina in materia di biometria e l'adozione biennale delle misure di garanzia disposte dall'art. 2-septies, sia possibile configurare nuovi illeciti e disporre una disciplina più puntale per l'adozione di misure di prevenzione e di un sistema cautelare per la tutela delle vittime.

[233] Vedere testo dell'art. 494 c.p.

[234] Cass. pen., 14 dicembre 2007, n. 46674, in Dir. Internet, 2008, 3, 249; Cass. pen., 3 aprile 2012, n. 12479, in CED Cassazione, 2012.

[235] Vedere il punto 7.4 "Falsificazione biometrica" delle Linee guida in materia di riconoscimento biometrico e firma grafometrica, Allegato A al Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.

CAPITOLO 3: I DATI BIOMETRICI NELL'ORDINAMENTO STATUNITENSE

"Scrivo per dare più forza al vostro futuro e alla causa morale della vostra generazione."

(Shoshana Zuboff, 2019)

1. La disciplina biometrica nell'era del "*Capitalismo della sorveglianza*"

Nell'analizzare l'evoluzione della disciplina sulla biometria all'interno della visione occidentale il contesto statunitense si rivela essenziale, in quanto gli Stati Uniti detengono ormai da tempo un'enorme influenza non solo nello sviluppo e nella commercializzazione delle tecnologie di identificazione biometrica, ma anche nella promozione di un acceso dibattito accademico e sociale sulle implicazioni legate all'adozione di questi sistemi. In particolare, nel 2019 la professoressa di Harvard Shoshana Zuboff pubblica il suo best-seller "*The Age of Surveillance Capitalism*", un'opera spartiacque in grado di introdurre un nuovo paradigma nel dibattito sul rapporto fra la nostra società e l'intelligenza artificiale. In essa S. Zuboff, tracciando l'evoluzione storica delle grandi aziende digitali americane (Google, Apple, Facebook, Amazon) le quali per prime hanno introdotto modelli di business basati sulla raccolta di dati personali, individua una nuova forma di accumulazione capitalistica in grado di impadronirsi dell'esperienza umana per trasformarla in dati sulle nostre abitudini, comportamenti e interazioni[236]. Questo fenomeno, che prende il nome di "*Capitalismo della sorveglianza"*, viene definito come "un nuovo ordine economico che sfrutta l'esperienza umana

[236] S. Zuboff, N. Möller, D. Murakami Wood, D. Lyon, *Surveillance Capitalism: An Interview with Shoshana Zuboff,* in *Surveillance & Society*, 2019, 17 (1/2), 257-266., p. 259-261.

come materia prima per pratiche commerciali segrete di estrazione, previsione e vendita"[237]. Alla base di questo nuovo ordine economico, che incarna l'evoluzione di un mercato digitale sempre più globale e interdipendente, vi sono dunque i dati personali raccolti da aziende private per fini commerciali. Infatti, sebbene questi dati siano generalmente impiegati per migliorare l'esperienza di prodotti e servizi da parte dei consumatori, se sottoposti a un ulteriore trattamento possono determinare quello che viene definito come un "*surplus comportamentale*", ossia un eccesso di dati in grado di pronosticare i nostri comportamenti futuri, nel breve e nel lungo periodo[238].

L'opera di S. Zuboff si rivela essenziale in quanto per prima pone una riflessione sullo sviluppo di un mercato digitale nel quale noi stessi diveniamo il principale oggetto di scambio, tramite la commercializzazione dei nostri dati personali. Il surplus comportamentale infatti si determina a partire dal recupero di dati comportamentali che, se una volta costituivano materia di scarto, ad oggi si rivelano riserve preziose ed estremamente profittevoli per le aziende, in quanto se sottoposti a processi di intelligenza artificiale, possono dar luogo a prodotti predittivi in grado di profilare in modo estremamente accurato i consumatori.

Di fatto, il cambiamento nell'uso di questi dati comportamentali ha posto le fondamenta per una nuova forma di mercato, il "*mercato dei comportamenti futuri*", di cui queste previsioni comportamentali costituiscono la valuta digitale del futuro[239]. L'accumulazione di dati personali che consentano di tracciare la nostra esperienza umana, partendo dalla nostra identità, abitudini di acquisto, fino al modo con cui costruiamo relazioni online, definisce pertanto in termini commerciali la nuova frontiera del capitalismo contemporaneo[240].

Queste tendenze contestualizzate in relazione ai dati biometrici si rivelano ancora più allarmanti, in quanto non solo assistiamo a sviluppi economici nei quali i nostri corpi divengono vere e proprie merci di scambio, ma tramite l'acquisizione di immagini facciali, profili biometrici, impronte digitali, è possibile detenere elementi essenziali dell'identità di un soggetto per finalità non solo commerciali, ma anche di controllo e di sorveglianza. L'impiego del surplus comportamentale ottenuto dalla rilevazione dei dati biometrici dei consumatori, rappresenta pertanto l'ultimo traguardo per questi innovativi modelli di business ormai sempre più pervasivi a livello globale. I sistemi di identificazione biometrica costituiscono la tecnologia più idonea a rilevare questi dati

[237] S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019, "La definizione".

[238] S. Zuboff, *Surveillance Capitalism anf the Challenge of Collective Action*, in *New Labor Forum*, 2019, Vol.28(I), p. 11-13.

[239] S. Zuboff, N. Möller, D. Murakami Wood, D. lyon, *Surveillance Capitalism: An Interview with Shoshana Zuboff*, in *Surveillance & Society*, 2019, 17 (1/2), p. 263-264.

[240] G. Tropea, *Recensione a S. Zuboff, Il Capitalismo della sorveglianza. Il futuro dell'umanità dell'era dei nuovi poteri, Roma, Luiss University Press, 2019 (con una postilla su Privacy e Covid-19)*, in *P.A. Persona e Amministrazione*, 2020, p. 480-481.

comportamentali, infatti già da tempo un numero sempre maggiore di rivenditori statunitensi, quali ad esempio i negozi Albertsons e Macy's[241], ammettono esplicitamente l'utilizzo del riconoscimento facciale per tracciare i profili dei loro consumatori, assieme alle loro abitudini di acquisto e prevenire possibili furti. Al fianco di questa nuova forma di accumulazione capitalistica emerge la questione della sorveglianza[242], infatti queste tecnologie predittive possono interferire notevolmente nella tutela della privacy delle persone coinvolte, mettendo in atto vere e proprie azioni di controllo e profilazione. I sistemi di rilevamento biometrico costituiscono la tecnologia più efficace per mettere in campo queste strategie di controllo, ma a quale prezzo? Da un lato, lo sviluppo di queste tecnologie consente l'adozione di sistemi di sicurezza estremamente efficaci per la prevenzione del crimine e il contrasto al terrorismo. Dall'altro dove non vi sono limiti chiari nel regolare l'uso di questi sistemi da parte del potere pubblico, vi è il rischio che questo potere possa rivelarsi arbitrario e tradire le sue finalità originarie di sicurezza e interesse pubblico[243].

Non bisogna al contempo dimenticare come lo sviluppo di queste tecnologie sia guidato prevalentemente dagli investimenti di grandi aziende digitali, le quali costituiscono alcuni dei pochi soggetti in grado in investire il capitale economico necessario a finanziare la ricerca in questo campo, mentre il settore pubblico dipende fortemente da questi attori privati per avervi accesso. Pertanto, se può ritenersi controversa l'affermazione di un monopolio privato sullo sviluppo di queste tecnologie, un loro utilizzo indiscriminato da parte dei pubblici poteri al di fuori di un sistema di regole chiaro, può rappresentare rischi maggiori per i diritti e le libertà dei cittadini. Per questo analogamente al caso europeo, anche negli Stati Uniti recentemente si è aperta una discussione sull'eventualità di apporre un vero e proprio divieto sull'uso del riconoscimento facciale all'interno degli spazi pubblici da parte di autorità di pubblica sicurezza, culminato nel novembre 2021 con l'approvazione a Bellingham (Washington) di un provvedimento per vietare l'impiego di tecnologie di riconoscimento facciale da parte delle autorità locali[244]. Quest'ultimo provvedimento si inserisce all'interno di una numerosa serie iniziata con una legge adottata a San Francisco nel 2019[245], che attualmente annovera circa due dozzine di provvedimenti analoghi[246].

---

[241] H. Towey, *The retail stores you probably shop at that use facial-recognition technology*, in *Business Insider*, 19 luglio 2021.
https://www.businessinsider.com/retail-stores-that-use-facial-recognition-technology-macys-2021-7?r=US&IR=T

[242] J. Andrew, M. Baker, *The General Data Protection Regulation in the Age of Surveillance Capitalism*, in *Journal of Business Ethics*, 2021, 168, p. 568-570.

[243] J. Cinnamon, *Social Injustice in Surveillance Capitalism*, in *Surveillance & Society*, 2017, 15(5), p. 610-612.

[244] T. Simonite, *Face Recognition Is Being Banned – but It's Still Everyehere*, in *Wired*, 22 dicember 2021.
https://www.wired.com/story/face-recognition-banned-but-everywhere/

[245] G. Barber, *San Francisco Bans Angency Use of Facial-Recognition Tech*,in *Wired*, 14 may 2019.
https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/

[246] Le normative più restrittive sul riconoscimento facciale negli Stati Uniti sono arrivate dai consigli comunali. In tutto il paese, i comuni hanno approvato leggi che vietano l'uso di tecnologie di riconoscimento facciale da parte di agenzie statali e locali, in particolare dipartimenti di polizia. Ad oggi, tali divieti sono stati approvati nelle città della California (Alameda, Berkeley, Oakland e San Francisco); Massachusetts (Boston, Brookline, Cambridge, Northampton, Somerville

La diffusione di una regolamentazione più ferrea sull'uso di questi sistemi biometrici da parte di pubblici poteri riflette la volontà di attivisti e accademici di limitare la progressiva affermazione di sistemi di intelligenza artificiale sempre più invasivi nella privacy dei cittadini e prevenire qualsiasi forma illecita di sorveglianza di massa, contraria a qualsiasi principio democratico.

Questa tendenza è stata avvalorata anche da numerose aziende private come Facebook, che recentemente ha adottato la decisione di ritirare il proprio sistema di riconoscimento facciale per identificare le persone ritratte in foto postate online, proprio per dar conto delle crescenti preoccupazioni manifestate dalla società[247]. Quando si analizza il contesto statunitense si assiste però a una forte contraddizione: se l'utilizzo di questi sistemi in ambito pubblico viene fortemente contestato, in ambito privato si riscontra invece un orientamento fondato prevalentemente su una forte deregolamentazione. Di fatto, attualmente negli Stati Uniti risulta del tutto assente una legge federale per la regolazione dei sistemi di riconoscimento biometrico e la loro disciplina viene definita prevalentemente tramite l'adozione di singole leggi nazionali (di cui attualmente si riscontra solo un numero esiguo in pochi stati) oppure in ambito giurisprudenziale (trovandosi all'interno di un sistema di common law). Tutto ciò concorre a definire un paradosso sostanziale nel quale se l'uso di questi sistemi viene generalmente bandito in contesti pubblici, viene invece sempre più normalizzato all'interno dei contesti privati più difficili da controllare in assenza di un chiaro quadro normativo di riferimento come nella disciplina sulla privacy europea.

Studiare i dati biometrici nell'ordinamento statunitense si rivela estremamente significativo in quanto non solo ci consente di elaborare la loro disciplina all'interno del contesto effettivo in cui si sono sviluppate queste tecnologie ed il loro mercato digitale, ma ci permette anche di analizzare un modello diametralmente opposto rispetto al contesto europeo, caratterizzato da un approccio maggiormente rivolto alla deregolamentazione di questi sistemi, con una disciplina sulla privacy decisamente meno articolata rispetto alla disciplina del GDPR europeo[248]. Negli Stati Uniti i privati hanno uno spazio di azione molto più ampio nell'adozione di questi sistemi biometrici e ciò spesso comporta pericolose zone d'ombra, difficili da controllare quando si tratta di tutelare i diritti delle persone indirettamente coinvolte. Infatti, in un sistema nel quale il trattamento dei dati biometrici da parte dei privati non è sempre fondato sul consenso esplicito dell'interessato come nel contesto europeo, diviene possibile

e Springfield); Jackson, Mississippi; King County, Washington; Portland, Maine; Portland, Oregon; Madison, Wisconsin; Minneapolis, Minnesota; Hamden, Connecticut; e New Orleans, Louisiana. Altre città, come Davis, California; Pittsburgh, Pennsylvania; e Nashville, nel Tennessee, hanno anche approvato ordinanze che regolano l'uso della tecnologia di sorveglianza tramite il riconoscimento facciale.

[247] K. Hill, R. Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, in *New York Times*, 5 november 2021.
https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html

[248] J. Andrew, M. Baker, *The General Data Protection Regulation in the Age of Surveillance Capitalism*, in *Journal of Business Ethics*, 2021, 168, p. 565-568.

adottare simili sistemi di controllo senza finalità di interesse pubblico e senza nemmeno che la persona ripresa sia a conoscenza della rilevazione alla quale è soggetta. Ciò ha da tempo alimentato un forte dibattito, caratterizzato dall'attività di numerosi attivisti che hanno dato vita a campagne quali "*Ban Facial Recognition in Stores"*[249], una campagna per limitare l'uso di sistemi biometrici all'interno di negozi per tracciare i consumatori per scopi commerciali. All'interno del sito di questa campagna è disponibile infatti un elenco dettagliato con numerose catene di negozi e la dicitura esplicita del se facciano o meno utilizzo del riconoscimento facciale, o se non sia specificato e quindi sia possibile che sia adottato in qualche misura. In questo modo i cittadini statunitensi possono scegliere consapevolmente quali rischi assumersi e come orientare le proprie strategie di acquisto in base alla trasparenza da parte dei rivenditori nell'utilizzo di questi sistemi.

Favorire strategie per incrementare i propri profitti rispetto alla tutela del diritto alla privacy dei cittadini, pone di fatto questioni etiche essenziali che differenziano notevolmente il paradigma statunitense da quello europeo. Nell'era del capitalismo della sorveglianza, si rende necessario dar conto dei rischi crescenti legati a queste tendenze. Di fatto l'emersione di queste riflessioni all'interno della dottrina statunitense non è casuale, ma è la diretta conseguenza di un processo di deregolamentazione che ha portato a porre in secondo piano la tutela della privacy dei cittadini rispetto al perseguimento di queste nuove forme di economia di mercato. L'opera di S. Zuboff mette in guarda rispetto al perseguimento di questo modello economico, anche se l'affermazione del capitalismo della sorveglianza viene descritta come un fenomeno ormai irreversibile e determinato a svilupparsi ulteriormente nei prossimi anni. Nei successivi paragrafi analizzeremo approfonditamente come l'elaborazione di una specifica disciplina statunitense sulla biometria possa ridurre l'effetto di queste tendenze introducendo maggiori tutele per i diritti e le libertà dei cittadini. Data la presenza crescente della biometria nella vita degli individui è necessaria una regolamentazione efficace che governi la sicurezza di questi sistemi e attribuisca ai consumatori una libertà di controllo sula propria privacy.

2. L'intervento del legislatore in materia di biometria

Il National Institute of Standards and Technology ("NIST")[250] definisce i dati biometrici come le misurazioni di caratteristiche fisiologiche come (ma non limitate a) impronte digitali, modelli dell'iride o caratteristiche facciali che possano essere utilizzate per identificare un individuo[251].

[249] Sito ufficiale della campagna Ban Facial Recognition in Stores. https://www.banfacialrecognition.com/stores/

[250] Il National Institute of Standards and Technology (NIST) è stato fondato nel 1901 e ora fa parte del Dipartimento del Commercio degli Stati Uniti. Il NIST è uno dei più antichi laboratori di scienze fisiche della nazione.

[251] National Institute of Standards and Technology, definition of "biometrics". https://perma.cc/52TG-8ATV

Tuttavia, nell'ambito della presente analisi abbiamo stabilito come le rilevazioni biometriche non si riferiscano solo a caratteristiche fisiologiche dell'individuo, ma anche a caratteristiche comportamentali, come l'espressività di un volto, la velocità con cui si appone una firma o la sonorità di una voce. L'autenticazione biometrica, definita come la misurazione delle caratteristiche fisiche e comportamentali misurabili di un individuo, non rappresenta un fenomeno recente negli Stati Uniti. Il governo e le forze dell'ordine lo usano da tempo. Il Federal Bureau of Investigation (FBI) ha creato un database di riconoscimento biometrico; il Dipartimento per la sicurezza interna degli Stati Uniti condivide l'iride e il riconoscimento facciale degli stranieri con l'FBI. Ma l'uso dei dati biometrici da parte dei produttori di beni di consumo per scopi di autenticazione è salito alle stelle negli ultimi anni[252]. Numerose aziende americane hanno contribuito enormemente nel rendere pervasivo l'uso di queste tecnologie nel nostro quotidiano. Ad esempio, Apple è stata una delle prime a implementare un sistema di rilevazione di impronte digitali (*Touch-ID*) e un sistema di riconoscimento facciale (*Face-ID*) all'interno dei suoi iPhone, per consentire lo sblocco del dispositivo, ma anche la possibilità di proteggere documenti sensibili o autenticare pagamenti online[253].

A causa del rapido sviluppo di queste tecnologie e della natura estremamente sensibile del dato biometrico, negli Stati Uniti si avverte sempre con maggiore urgenza l'esigenza si introdurre una regolazione federale di questi sistemi, per individuare degli standard uniformi nella tutela della privacy dei consumatori[254]. Infatti, l'approccio statunitense nella regolazione queste tecnologie riflette una politica liberista volte a prediligere un approccio "*laissez fare*", piuttosto che un intervento mirato con una rigida disciplina sulla privacy che rischi di ingessare il mercato digitale. La tutela dei diritti del soggetto privato si determina prevalentemente in funzione della facilitazione di queste dinamiche di mercato, non prevedendo una regolazione federale sulla biometria e lasciando un ampio spazio di autonomia ai singoli stati. In generale, la disciplina sulla privacy è un'area emergente del diritto statunitense che manca di una regolamentazione standardizzata a livello federale[255]. I principali istituti sulla privacy attualmente in vigore sono le leggi federali, quali il *Federal Trade Commission Act* (FTC)[256], il *Gramm-Leach-Bliley Act* (GLBA)[257] e l'*Health Insurance Portability and Accountability Act* (HIPAA)[258]. Il comune denominatore alla base di queste leggi sulla privacy è l'adozione delle *Fair Information Practices* (FIPs), ossia la diffusione di pratiche informative volte

[252] N. Memon, *How Biometric Authentication Poses New Challenges to Out Security and Privacy*, in *IEE Signal Processing Magazine*, Vol. 4, n. 4, 2017, p. 194-196.
[253] A. Bud, *Facing the future: the impact of Apple FaceID*, in *Biometric Technology Today*, n. 1, 2018, p. 5-7.
[254] F. Q. Nguyen, *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, Vol. 7., n. 1, 2018, p. 67-71.
[255] S. M. Boyne, *Data Protection in the United States*, in *The American Journal of Comparative Law*, 2018, p. 300-303.
[256] Federal Trade Commission Act, Incorporating U.S. Safe Web Act amendments of 2006, 15 U.S.C. §§ 41-58, as amended.
[257] Gramm-Leach-Bliley Act, Public Law 106 – 102 – Nov. 12, 1999.
[258] Health Insurance Portability and Accountability Act, Public Law 104 – 191 – Aug. 21, 1996.

a favorire una corretta informazione sulla privacy all'interno del mercato per le comunicazioni elettroniche, che prevedano l'adozione di istituti quali l'informativa e il consenso. Nessuno di questi strumenti normativi dispone però una disciplina puntale sulla raccolta e l'utilizzo di dati biometrici e solo l'FTC, seppur non li regoli direttamente, ha promulgato una lista di pratiche consigliate per la rilevazione e la conservazione dei dati biometrici di un soggetto[259]. Pertanto, l'attuale quadro giuridico statunitense sull'identificazione e autenticazione di dati biometrici è caratterizzato esclusivamente dall'adozione di singole leggi statali. Infatti, nonostante il Congresso debba ancora emanare una regolazione federale, per quanto concerne la protezione e l'uso della biometria alcuni stati hanno già preso autonomamente una propria iniziativa sulla questione, guidando un movimento necessario. Come vedremo nei successivi paragrafi attualmente negli Stati Uniti esistono unicamente tre leggi nazionali in materia di biometria promulgate dagli stati dell'Illinois, Texas e Washington, a cui deve essere aggiunta l'esperienza del *California Consumer Privacy Act* e di alcuni disegni di legge in corso di elaborazione in altri stati. Anche il *Commercial Facial Recognition Act* proposto nel 2019 da due senatori statunitensi, ha segnato un'esperienza significativa nel percorso per l'istituzione di una regolazione federale in materia di biometria.

2.1 La legislazione statale sui dati biometrici

Mentre la società statunitense continua a sviluppare le tecnologie biometriche, per comprendere i modelli di regolazione adottati a livello nazionale attualmente in vigore è necessario riconoscere la differenza tra sistemi di identificazione biometrica e sistemi di autorizzazione biometrica. Il legislatore statunitense, infatti, generalmente distingue fra identificazione e autenticazione biometrica. Gli identificatori biometrici sono tratti della persona come l'iride, la voce o le impronte digitali, pertanto l'identificazione biometrica può essere descritta come l'utilizzo dell'identificatore biometrico di un individuo per abbinare il tratto rilevato con quello precedentemente conservato all'interno di un database, per effettuarne un corretto riconoscimento. L'autenticazione biometrica invece, al contrario, prevede che l'individuo sia in grado di dimostrare la sua identità attraverso la scansione di un suo tratto biometrico che, una volta confrontato con un identificatore precedentemente rilevato, ne autorizza l'accesso ad aree e contenuti sensibili. Seppur simili, questi due approcci nella lettura dei sistemi di identificazione biometrica riflettono orientamenti nelle strategie di *policy making* in parte difformi[260]. Infatti, alcune delle leggi statali in materia di biometria

[259] Federal Trade Commission, Privacy and Data Security Update Report, 2018. Le FCT's best practices riguardano misure in materia di trasparenza, privacy by design e semplificazione della scelta del consumatore.
[260] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, cit., p. 232-233.

statunitensi regolano in modo diverso i sistemi di identificazione biometrica rispetto ai sistemi di autorizzazione biometrica, concentrandosi spesso solo su di una delle due strategie di riconoscimento biometrico. Oltre a questo aspetto, l'adozione di un modello di legislazione "*State by State*" che prevede l'elaborazione di singole leggi nazionali per la protezione dei dati biometrici, pone ulteriori ostacoli all'adozione di una strategia uniforme nella regolazione di questi sistemi[261]. I procedimenti legislativi statali, di fatto, risultano spesso troppo lenti rispetto alla velocità con cui queste tecnologie si sviluppano. Inoltre, gli strumenti adottati per tutelare la privacy dei cittadini di uno stato potrebbero danneggiare i consumatori residenti in altri stati con leggi per la protezione dei dati personali più deboli, oppure un'azienda potrebbe decidere di investire le sue risorse solo all'interno di stati privi di leggi in materia di biometria. Queste situazioni tendono a verificarsi in due casi, sia quando alcuni stati adottano queste previsioni a discapito di altri, che quando uno stato adotta degli standard di regolazione molto più stringenti di altri. Di conseguenza, nel tempo gli stati più lenti nel legiferare si riveleranno più vulnerabili al trattamento dei dati biometrici non protetto, mentre le aziende che hanno consumatori in più stati faranno fatica a conformarsi a una legislazione confusa e gravosa. Invece, ciò non si verificherebbe se vi fosse un comune standard minimo federale da rispettare per le aziende e i tribunali di ogni stato. Di seguito analizzeremo in dettaglio la normativa attualmente in vigore all'interno dei singoli stati statunitensi.

2.1.1 Il *Biometrics Information Privacy Act* in Illinois

Nel 2008 lo stato dell'Illinois ha adottato una legge in materia di protezione dei dati personali, il *Biometrics Information Privacy* Act[262], noto anche con il nome "Illinois BIPA", che include una disciplina per la raccolta e conservazione dei dati biometrici. L'intento di questo intervento normativo era porre una tutela concreta della privacy dei cittadini, rispetto alla raccolta di questi sensibili. All'interno dell'Illinois BIPA i dati biometrici sono suddivisi in identificatori biometrici (*biometric identifiers*) e informazioni biometriche (*biometric informations*)[263].

Nel primo caso, si fa riferimento ai singoli caratteri biometrici dell'individuo, quali la retina o l'impronta digitale[264], mentre nel secondo si ritiene un'informazione biometrica qualsiasi informazione ricavata dalla rilevazione di un identificatore biometrico, utilizzata per identificare un

[261] F. Q. Nguyen, *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, cit., p. 71-72.
[262] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15, 2008.
[263] H. Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, in *University of Kansas Law Review*, 66, 2018, p. 648-651.
[264] Ai sensi della sezione § 10 BIPA, sono espressamente esclusi tra gli identificatori biometrici: i campioni di scrittura; la firma; le fotografie; campioni biologici umani raccolti per finalità di ricerca; i dati demografici; descrizioni di tatuaggi; o descrizioni fisiche come l'altezza, il colore degli occhi o dei capelli.

individuo[265]. Inoltre, all'interno della legge viene definita come informazione sensibile, qualsiasi dato personale che possa essere utilizzato per identificare in modo univoco un individuo. La sezione 15 dell'Illinois BIPA stabilisce in dettaglio le misure per la rilevazione, la conservazione, la divulgazione e l'eliminazione sia degli identificatori biometrici che delle informazioni biometriche[266]. Per far sì che un'azienda possa disporre in modo lecito il trattamento di identificatori e informazioni biometriche, viene richiesta la predisposizione di un'apposita informativa contenente le informazioni sul programma di conservazione e le linee guida per la successiva eliminazione dei dati raccolti, una volta che lo scopo del trattamento sia stato raggiunto[267]. Inoltre, prima di effettuare una qualsiasi forma di trattamento deve essere trasmessa una comunicazione esplicita al soggetto coinvolto, spiegando la natura della rilevazione alla quale sarà sottoposto. L'individuo o il suo rappresentante legale deve essere informato in modo scritto del trattamento e della conservazione dei propri dati biometrici. L'informativa deve inoltre contenere nello specifico anche lo scopo della raccolta, la sua durata e le modalità di conservazione. Quindi qualsiasi ente o azienda privata deve fornire una comunicazione scritta all'individuo, prima di disporre la raccolta dei dati.

All'interno della medesima sezione vengono stabiliti anche dei limiti espliciti per la divulgazione di queste informazioni sensibili e l'Illinois BIPA scoraggia esplicitamente le aziende private dal trarre profitto dalla raccolta di queste tipologie di dati. Infatti, la legge vieta espressamente la divulgazione degli identificatori o delle informazioni biometriche, a meno che non sia presente il consenso esplicito da parte dell'individuo. Oltre al consenso, la divulgazione di questi dati è consentita solo nei casi in cui l'individuo completi una transazione finanziaria autorizzata, oppure in cui vi sia l'esplicito mandato o la citazione emessa da un tribunale[268]. Ogni ente o azienda privata che disponga un trattamento di dati biometrici deve, inoltre, aderire a degli standard precisi durante la raccolta e la conservazione di questi dati sensibili. In tal senso, l'Illinois BIPA dispone che l'ente privato debba tutelare i dati biometrici con i medesimi standard di sicurezza con cui dispone la conservazione e il trasferimento di informazioni confidenziali e sensibili.

Uno degli aspetti più interessanti della legge è che, all'interno della sezione 20, riconosce al privato la possibilità di intraprendere un'azione legale in un tribunale statale o come richiesta supplementare presso il tribunale distrettuale federale, qualora risulti parte lesa per una violazione delle sue

[265] Ai sensi della sezione § 10 BIPA, le informazioni biometriche possono essere acquisite per mezzo della rilevazione, conversione, archiviazione o condivisione dell'identificatore biometrico di un individuo. Tuttavia, viene delineato espressamente come qualsiasi informazione proveniente dalla lista di identificatori esclusi non possa essere classificata come un'informazione biometrica.

[266] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, cit., p. 240.

[267] Ai sensi della sezione § 10 BIPA, è necessario che l'ente privato aderisca al suo programma di conservazione e successiva eliminazione del dato biometrico, entro tre anni dall'ultimo contatto con l'individuo a cui appartiene il dato.

[268] Ai sensi della sezione § 15 BIPA, che dispone per gli enti privati il divieto di vendere, commercializzare o trarre profitto da identificatori o informazioni biometriche.

disposizioni[269]. Infatti la normativa non solo dispone per l'individuo, soggetto alla violazione, la possibilità di richiedere un risarcimento per i danni, ma gli attribuisce anche la possibilità di ottenere il rimborso delle proprie spese legali e altre forme di risarcimento[270]. In particolare, l'entità dei danni a cui la parte lesa può avere diritto viene stimata a partire dai mille fino ai cinquemila dollari, se l'ente privato ha agito deliberatamente in modo doloso. Da ultimo, è importante sottolineare come l'Illinois BIPA si astenga dell'interferire con l'ammissione o la rilevazione di identificatori o informazioni biometriche per scopi investigativi in ambito processuale. La legge dell'Illinois infatti, ai sensi della sezione 25, non può interferire con alcuna normativa federale e non può applicarsi ad alcuna agenzia statale o unità governativa locale.

2.1.2 Il *Legislative House Bill 1493* di Washington

Lo stato di Washington ha adottato nel 2017 il *Legislative House Bill 1493*[271], noto anche come "H.B. 1493", introducendo delle misure specifiche per la protezione degli identificatori biometrici. In questo caso, infatti, non viene disposta la differenziazione tra indicatori biometrici e informazioni biometriche. L'H.B. 1493 definisce come identificatore biometrico[272] "la misurazione automatica delle caratteristiche biologiche di un individuo" nella forma di dati[273].

Nello specifico questo intervento normativo stabilisce che all'individuo soggetto al trattamento debba essere fornito un ragionevole preavviso prima di disporre la raccolta del dato biometrico. Inoltre, è necessario che l'individuo fornisca il suo consenso al trattamento. La predisposizione degli obblighi di informativa e consenso riflette la volontà del legislatore di vincolare le imprese alla predisposizione di informazioni chiare e trasparenti sulla natura dei loro trattamenti commerciali, tutelando la privacy dei loro consumatori[274]. Pertanto, per registrare legalmente un identificatore biometrico in un database per scopi commerciali, un ente privato deve fornire un'informativa e ottenere il consenso del soggetto interessato. Inoltre, viene richiesta anche la predisposizione di un meccanismo per prevenire successivamente che il dato sia nuovamente utilizzato per ulteriori scopi commerciali. Infatti, solo dopo che un identificatore biometrico è stato registrato all'interno di un database per

[269] A. L. Metzger, *The Litigation Rollercoaster of BIPA: A comment on the Protection on Individuals from Violations of Biometric Information Privacy*, in *University of Chicago Law Journal* , n. 50, 2019, p. 1064-1068.
[270] Ai sensi della sezione § 20 BIPA, che concede alla parte lesa il risarcimento di spese legali ragionevoli, incluse le spese per l'acquisizione di periti e le spese per sostenere il contenzioso.
[271] Legislative House Bill 1493, 65th Leg., Reg. Sess., Washington, 2017.
[272] L'H. B. esclude dalla categoria degli identificatori biometrici: le fotografie; registrazioni video o audio, compresi i dati ricavabili da essi; informazioni e dati raccolti all'interno di trattamenti sanitari.
[273] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation,* cit., p. 242.
[274] M. J. Anderson, J. Halpert, *Washington Becomes the Third State with a Biometric Privacy Law: Five Key Differences,* in *RAIL: The Journal of Robotics, Artificial Intelligence & Law*, 1(1), 2018, p. 42-43.

scopi commerciali l'H.B. 1493 ne vieta la vendita, lo spostamento o la divulgazione a meno che non sia presente il consenso dell'interessato. La legislazione di Washington risulta, tuttavia, più indulgente rispetto al modello dell'Illinois BIPA, in quanto fornisce degli standard di sicurezza differenti a seconda che l'identificatore biometrico sia acquisito o registrato[275]. Sebbene siano necessari l'informativa e il consenso per registrare l'identificatore biometrico di un soggetto, di fatto, vi sono situazioni nelle quali un ente privato può rivelare gli identificatori biometrici a terzi senza raccogliere il consenso dell'interessato.

Il consenso alla divulgazione può non essere fornito nei casi in cui: la divulgazione del dato è necessaria per erogare un prodotto o servizio all'interessato, oppure per facilitare un'operazione finanziaria richiesta e autorizzata dal soggetto; o autorizzata da uno statuto federale o statale o da un'ingiunzione del tribunale, necessaria per preparare il contenzioso, oppure se la divulgazione viene effettuata da una terza parte che contrattualmente accetta che l'identificatore biometrico non sia ulteriormente divulgato o registrato per uno scopo commerciale.

Se una terza parte accetta contrattualmente di non divulgare un identificatore biometrico, tale terza parte sarà comunque tenuta a seguire le regole di avviso e consenso qualora essa intenda utilizzarlo per scopi commerciali. Inoltre, un ente privato che disponga la registrazione di un identificatore biometrico di un individuo per uno scopo commerciale o ottenga l'identificatore biometrico di un individuo da una terza parte per uno scopo commerciale, non può divulgarlo se è contrario allo scopo iniziale per cui è stato raccolto, a meno che la persona non ottenga il consenso dell'interessato per le nuove condizioni di utilizzo o divulgazione. Da ultimo, i presupposti di informativa e consenso non sono necessari qualora si effettui una semplice acquisizione dell'identificatore biometrico, anche per scopi commerciali, ma senza portare a una sua registrazione o qualora la raccolta si renda necessaria per finalità di sicurezza. L'H.B. 1493 non riconosce al privato la possibilità di intraprendere un'azione legale come nel modello dell'Illinois BIPA, pertanto un'azione legale può essere intentata soltanto dal procuratore generale ai sensi della legge sulla protezione dei consumatori di Washington. Inoltre, questa normativa non può applicarsi alla legislazione federale e interferire nell'ambito delle competenze delle forze di pubblica sicurezza.

In conclusione, il modello dell'H.B. 1493 si rivela come più favorevole alle imprese rispetto al modello dell'Illinois BIPA, in quanto si tratta di un modello esclusivamente rivolto all'ambito commerciale e più permissivo in merito alla raccolta di informazioni biometriche[276]. Infatti, rispetto

[275] L'H. B. 1493 definisce la registrazione dell'identificatore biometrico, come il processo di rilevazione di un dato biometrico individuale, convertendolo in un modello di riferimento che non può essere ricostruito a partire dall'output originale e archiviandolo in un database che abbini l'identificatore al soggetto specifico. L'acquisizione dell'identificatore biometrico concerne, invece, il semplice processo di estrapolazione del dato dall'individuo.

[276] D. Taneja, *Whasington Enacts a Biometric Privacy Statute in a Departure from the Existing Standard*, in *New Media and Technology Law Blog*, 13 giugno 2017. https://perma.cc/6F2X-27CA

al secondo, nel modello H. B. 1493 è possibile disporre la raccolta di dati biometrici per scopi commerciali senza il consenso dell'interessato se il dato viene solo acquisito ma non registrato, lasciando dei margini di autonomia molto più ampi per le aziende private[277].

2.1.3 Il *Capture or Use of Biometric Identifier Act* in Texas

Nel 2009, un anno dopo l'approvazione dell'Illinois BIPA, anche il Texas ha adottato una legge in materia di biometria, attraverso l'approvazione del capitolo 503, 11, sottotitolo A, del *Business and Commerce Code*, noto come *the Capture or Use of Biometric Identifier Act*[278] e abbreviato in "CUBI Act". Anche nel modello adottato dal Texas non è presente una definizione specifica per le informazioni biometriche, occupandosi solo degli identificatori biometrici.
In particolare, il CUBI Act definisce l'identificatore biometrico, analogamente all'Illinois BIPA, come un carattere biometrico quale la scansione della retina, delle impronte digitali, del timbro vocale, o dei tratti del volto (anche se le fotografie e le registrazioni video restano escluse da questa definizione). Rispetto all'H.B. 1493, invece, il modello texano introduce i parametri dell'informativa e del consenso anche in riferimento alla rilevazione degli identificatori biometrici per scopi commerciali[279]. Infatti, quest'ultimi vengono estesi anche alla mera raccolta di dati biometrici, senza una loro successiva registrazione. In riferimento alla vendita, divulgazione e circolazione degli identificatori biometrici per scopi commerciali, queste azioni vengono in linea di principio vietate a meno che non sussista una delle presenti condizioni[280]:

- L'individuo presta il consenso alla divulgazione per finalità identificative in caso di morte o di persona scomparsa;
- La divulgazione del dato è finalizzata al completamento di una transazione finanziaria che l'individuo ha richiesto o autorizzato;
- La divulgazione è richiesta o autorizzata da una legge federale o da una legge statale;
- La divulgazione viene condotta da un'autorità di pubblica sicurezza in applicazione della legge, previo mandato.

[277] M. J. Anderson, J. Halpert, *Washington Becomes the Third State with a Biometric Privacy Law: Five Key Differences*, cit., p. 44-45.
[278] Tex. Bus. & Com. Code Ann. § 503.001, 2009.
[279] T. Claypoole, C. Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, in *Business Law Today*, n. 5, 2016, p. 2-3.
[280] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, cit., p. 245.

Uno dei punti di forza del CUBI Act rispetto ai modelli adottati negli altri stati, è la velocità con cui dispone l'eliminazione dei dati raccolti. Infatti, successivamente al primo anniversario della scadenza della finalità per cui il dato biometrico era stato raccolto, l'ente privato deve disporre l'eliminazione dell'identificatore. Tuttavia, se la legge richiede che la conservazione del dato decorra per un periodo di tempo più esteso, il termine può non essere rispettato. Nei trattamenti di dati biometrici nei rapporti di lavoro il termine per la rimozione dei dati ricorre in concomitanza con la conclusione del rapporto di lavoro. Da ultimo, anche in questo caso seppur vengano riconosciute delle sanzioni civili, il procuratore generale è l'unico soggetto autorizzato a far valere un'azione legale. Pertanto, il soggetto privato anche se colpito direttamente da una violazione non può presentare un'azione legale. Dei casi fin qui analizzati, l'Illinois BIPA risulta il modello con gli standard di sicurezza più alti nel disciplinare il trattamento di dati biometrici, essendo anche l'unico stato che attribuisce direttamente al soggetto interessato la possibilità di intraprendere un'azione legale per poter far valere i propri diritti.

2.1.4 La legislazione in materia di privacy biometrica in California e Arkansas

Il 9 agosto 2019, l'Arkansas ha modificato la definizione di dato personale all'interno della propria legge in materia di violazione dei dati personali per includervi i dati biometrici[281]. In essa, i dati biometrici sono identificati come la rilevazione di caratteri biologici come il timbro vocale, l'impronta della mano, l'impronta digitale, il DNA, la scansione della retina/iride, la geometria della mano o l'impronta facciale, finalizzata all'autenticazione univoca dell'identità di un soggetto. Ai sensi della legge dell'Arkansas, le aziende e le persone che acquistano, possiedono o concedono in licenza dati personali, compresi i dati biometrici, sono tenuti a rispettare pratiche di sicurezza ragionevoli e appropriate per proteggere i dati da fonti di accesso e mezzi di divulgazione non autorizzati. In caso di violazione dei dati, le aziende sono quindi tenute a informare le persone interessate della violazione avvenuta e nel caso in cui il numero delle persone coinvolte sia maggiore a mille, la segnalazione deve essere fatta anche al procuratore generale.

Nel 2018, invece, lo stato della California ha adottato il *California Consumer Privacy Act* (CCPA)[282], ampliando il proprio quadro normativo sulla privacy per ricomprendervi i dati biometrici[283]. Infatti, la legge entrata in vigore solo nel gennaio 2020, adotta anche un focus specifico sulle informazioni biometriche raccolte per scopi commerciali, ricomprendendo i dati biometrici all'interno della

[281] D. L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, in *Santa Clara High Technology Law Journal*, 38 (1), 2021, p. 82.
[282] Cal. Civ. Code § 1798.198(a), 2018.
[283] F. Q. Nguyen, *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, cit., p. 67.

categoria generale di dati personali raccolti per determinare il profilo di un consumatore[284]. Le informazioni biometriche raccolte per scopi non commerciali di fatto non sono sottoposte alla disciplina del CCPA. Ai sensi della legge californiana, i consumatori devono ricevere una notifica per ogni eventuale modifica apportata alla politica aziendale in materia di trattamento dei dati personali nell'arco dell'ultimo anno.

Inoltre, i consumatori devono avere strumenti chiari e semplici da utilizzare per potersi relazionare con l'azienda e poter richiedere che i propri dati non siano venduti a soggetti terzi. Infatti, questo tipo di richiesta deve provenire direttamente dal soggetto interessato, anche se nel CCPA si dispone che anche un soggetto terzo autorizzato possa intervenire per conto dell'interessato. Le aziende, di fatto, sono responsabili non solo delle informazioni biometriche di cui dispongono, ma anche di tutte le informazioni personali ad esse connesse che trasmettono ad aziende analoghe. Nel caso di una richiesta di cancellazione del dato, l'azienda dovrà eliminare ogni informazione personale del soggetto richiedente, invitando anche gli eventuali fornitori di servizi coinvolti nel trattamento a fare altrettanto. Pertanto, il CCPA richiede implicitamente alle aziende di tenere traccia degli enti o le imprese alle quali forniscono informazioni personali e di fornire a terzi un avviso qualora il consumatore dovesse modificare qualsiasi autorizzazione al trattamento[285].

Per quanto concerne la tutela dell'individuo rispetto a possibili illeciti, a differenza dell'Illinois Act, il CCPA dispone la possibilità di intraprendere azioni legali solo sulla base di alcune tipologie di violazioni individuate in modo specifico. Inoltre, il procuratore generale può intentare una causa se l'azienda non pone rimedio alla violazione segnalata entro il termine di 30 giorni, mentre l'individuo può agire solo nei casi limitati a violazioni connesse ad accessi non autorizzati o forme di infiltrazione, furto e divulgazione di dati personali in forme non crittografate o non oscurate. Le sanzioni previste sono analoghe a quelle predisposte dall'Illinois BIPA. Se il consumatore nega il suo consenso, l'azienda deve attendere almeno un anno prima di sottoporgli nuovamente un'autorizzazione alla vendita dei propri dati personali[286].

In conclusione, il California Consumer Privacy Act con la sua recente entrata in vigore sembrava pronto a oscurare la salienza del modello dell'Illinois BIPA. Molti osservatori si aspettavano, infatti, che il CCPA fungesse da nuova base nazionale per disciplina sulla privacy delle informazioni biometriche, date le dimensioni della California e la sua importanza economica[287]. La maggior parte

[284] E. M. Ghelardi, *Closing the Data Gap: Protection Biometric Information under the Biometric Information Privacy Act and the California Consumer Protection Act,* in *St. John's Law Review*, 94(3), 2020, p. 882-885.
[285] S. L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States,* in *Journal of Technology Law & Policy*, 23(1), 2020, p. 88-100.
[286] E. Goldman, *An Introduction to the California Consumer Privacy Act (CCPA),* in *Santa Clara Univ. Legal Studies Research Paper*, 2020, p. 5-7.
[287] S. Shatz, S. E. Chylik, *The California Consumer Privacy Act of 2018: A Sea Change in The Protection of California Consumers' Personal Information,* in *Business LAw.*, 75, 2020, p. 1919-1924.

delle aziende tecnologiche ha infatti sede nella Silicon Valley, dove gli esperti del settore prevedevano che le aziende interessate dalla nuova legge avrebbero fornito protezione a livello di CCPA direttamente a tutti i loro consumatori statunitensi, mentre invece la maggior parte delle aziende ha scelto di concedere la tutela del CCPA solo ai californiani, limitando fortemente l'espansione del suo modello. Il CCPA garantisce ai consumatori maggiori informazioni e controllo sulle loro informazioni biometriche, tuttavia rispetto al modello dell'Illionois BIPA, le violazioni in esso individuate consentono di rappresentare legalmente solo gli interessi di "consumatori", limitando la sua azione risarcitoria. Date le pesanti multe inflitte per aver violato le previsioni di legge, tuttavia, le aziende probabilmente interpreteranno la categoria di "consumatore" in modo ampio per evitare di incorrere in numerose azioni legali.

2.1.5 Proposte di legge in materia di privacy biometrica a New York e nel Maryland

Il 6 gennaio 2021 i rappresentanti dello stato di New York hanno proposto l'*Assembly Bill 27* (AB 27), ossia un disegno di legge per introdurre una disciplina in materia di biometria, noto come il *New York Biometric Privacy Act*[288]. L'obiettivo di questa proposta di legge è far si che le aziende private abbiano delle strette previsioni alle quali attenersi in materia di conservazione dei dati biometrici. Per questo il disegno prevede che le organizzazioni private non governative, nel disporre queste tipologie di trattamento, adottino un'informativa scritta che specifichi le misure adottate per la conservazione dei dati, lo scopo iniziale della loro raccolta e quando tale scopo può dirsi soddisfatto. Infatti, una volta raggiunto lo scopo perseguito, l'ente privato è obbligato a disporre l'eliminazione del dato raccolto entro tre anni dall'ultima interazione con l'individuo interessato[289].

Poco dopo la proposta dello stato di New York, anche il Maryland ha introdotto il suo *House Bill 218,* denominato "*Commercial Law Consumer Protection – Biometric Identifiers and Biometric Information Privacy*", proponendo un disegno di legge che ricalca quasi perfettamente il modello dell'Illinois BIPA. Infatti, anche la proposta di legge del Maryland istituisce per il privato la possibilità di ricorrere ad azioni legali e riconosce al ricorrente il rimborso delle spese legali sostenute, qualora il contenzioso abbia esito positivo. In questo caso, come nell'Illinois, l'introduzione di una simile legge potrebbe determinare una forte crescita nel numero di azioni collettive intraprese, obbligando le aziende private ad adottare cautele specifiche per evitare il rischio sempre maggiore di

[288] K. L. Lust, M. Galibois, J. Lefebvre, *New York proposes a new Biometric Privacy Act*, in *Technology Law Dispatch*, 11 gennaio 2021. https://www.technologylawdispatch.com/2021/01/privacy-data-protection/new-york-proposes-a-new-biometric-privacy-act/

[289] D. L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, cit., p. 82-84.

azioni collettive in futuro[290]. Inoltre, pure il disegno di legge del Maryland impone alle imprese l'adozione dei requisiti di informativa e consenso per disporre l'acquisizione, la raccolta e l'archiviazione di dati biometrici, dispone l'adozione di standard elevati di sicurezza nella conservazione dei dati e vieta categoricamente la divulgazione dei dati senza consenso. L'unica differenza fra l'Illinois BIPA e la proposta di legge del Maryland concerne la definizione di identificatori e informazioni biometriche. Mentre ai sensi del disegno di legge, gli identificatori biometrici sono definiti analogamente all'Illinois BIPA, come i dati relativi alle caratteristiche biologiche di un soggetto, ricavati attraverso sistemi di rilevazione automatizzati (quali la scansione dell'iride, le impronte digitali, il timbro vocale), nel modello adottato dal Maryland, le informazioni biometriche ottengono una definizione più ampia, atta a ricomprendere qualsiasi informazione che possa essere utilizzata per identificare un individuo, indipendentemente da dove sia stata ottenuta. Tuttavia, non rientra nella definizione di informazione biometrica qualsiasi informazione ricavata da un identificatore escluso dalla definizione di identificatore biometrico, quali le fotografie e i dati sanitari. Da ultimo, la proposta di legge del Maryland stabilisce che un'azienda possa anche non applicare le sue disposizioni, qualora il trattamento di dati biometrici sia applicato solo ai dipendenti di un ente privato per uso interno.

2.2 Il *Commercial Facial Privacy Act* del 2019

Nel marzo 2019, il senatore del Missouri Roy Blunt e il senatore delle Hawaii Brian Schatz hanno presentato il *Commercial Facial Privacy Act*[291], un progetto di legge orientato a porre le basi per una legislazione federale sull'uso del riconoscimento facciale[292]. L'obiettivo del disegno di legge era ponderare i vantaggi senza precedenti legati all'uso del riconoscimento facciale con la predisposizione di tutele specifiche per salvaguardare la privacy dei consumatori[293]. In particolare, all'interno di esso venivano predisposte una serie di misure per vietare ai soggetti commerciali l'uso della tecnologia biometrica per il riconoscimento facciale, senza aver ottenuto il consenso dell'utente per una finalità specifica[294].

---

[290] T. Ahlering, G. Maatman, *Maryland Joins Growing Number of States Introducing Biometric Information Privacy Bills With Potential to Spur Class Action Litigation*, in *JDSUPRA*, 24 febbraio 2021. https://www.jdsupra.com/legalnews/maryland-joins-growing-number-of-states-3182422/

[291] Commercial Facial Recognition Privacy Act, S. 847, 116th Cong., 2019.

[292] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, cit., p. 255-257.

[293] L. P. Angeles, *Untang Me: Why Federal Judges Are Broadly Construing Illinois's Biometric Privacy Law,* in *Cardozo Law* Review, 42(1), p. 356-357.

[294] Press relase, *Blunt, Schatz introduce bipartisan commercial facial recognition privacy act*, in *Roy Blunt Unites States Senator for Missouri* (sito ufficiale), 14 marzo 2019. https://perma.cc/9LMQ-MSRB

Infatti, uno dei suoi punti di forza era la predisposizione per il titolare del trattamento dell'obbligo di ottenere il consenso esplicito dell'utente prima di procedere nella raccolta dei dati sensibili e l'introduzione del divieto categorico di diffusione del dato biometrico raccolto senza il consenso dell'interessato. Inoltre, la proposta del *CFRP Act* mirava a proteggere i consumatori non solo dai rischi per la tutela della loro privacy, ma anche dagli effetti discriminatori che spesso possono emergere dall'uso di queste tecnologie, stabilendo per le aziende la necessità di effettuare test indipendenti per verificare la correttezza di questi sistemi, riducendo al minimo i rischi di discriminazione per gli individui. In molti casi, infatti, questi sistemi di riconoscimento identificano erroneamente i soggetti o possono determinare forme di pregiudizio[295] nella rilevazione di persone di colore, donne, anziani e disabili. In termini di applicazione, il disegno di legge conferiva alla Federal Trade Commission e ai procuratori generali dello stato la possibilità di presentare reclami ai sensi della legge. Invece, per quanto concerne le norme per la sicurezza dei dati e gli standard per la loro conservazione, la proposta di legge attribuiva alla FTC e al National Institute of Standards and Technology il compito di adottarli. Tuttavia, nonostante questa proposta di legge fosse stata introdotta nel marzo 2019 nell'ambito delle attività della legislatura 116th del Congresso (2019-2021) non è mai stata votata facendo fallire il progetto normativo dei due senatori statunitensi. Sebbene questo disegno di legge non sia stato emanato, però, le sue disposizioni sarebbero potute divenire legge se fossero state incluse in un altro disegno di legge. È prassi comune negli Stati Uniti che un testo legislativo sia introdotto contemporaneamente in più progetti di legge, detti progetti di legge complementari, per reintrodurlo nelle sessioni successive del Congresso.

3. Il contributo della giurisprudenza dello stato dell'Illinois

Abbiamo visto come in assenza di uno standard nazionale, l'adozione di un modello di legislazione stato-per-stato possa rilevarsi controversa nella predisposizione di una disciplina uniforme in materia di biometria[296]. In particolare, essendo l'Illinois BIPA la legge in materia di biometria che attualmente attribuisce al soggetto privato la forma più estesa di tutela legale, avendo introdotto per prima l'adozione di rimedi specifici e la possibilità di intraprendere un'azione legale per l'interessato, la si può ritenere il modello di legislazione più strutturato rispetto ai casi fin qui analizzati. In questa sezione, pertanto, saranno discussi alcuni celebri casi emersi in relazione all'applicazione dell'Illinois BIPA, che ne hanno plasmato l'interpretazione da un punto di vista giurisprudenziale[297].

[295] F. Bacchini, L. Lorusso, *Race, again: how face recognition technology reinforces racial discrimination*, in *Journal of Information, Communication and Ethics in Society*, Vol. 17(3), 2019, p. 321-323.
[296] F. Q. Nguyen, *The Standard for Biometric Data Protection,* in *Journal of Law & Cyber Warfare*, cit., p. 67.
[297] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation,* cit., p. 246-252.

3.1 Il caso *Rosenbach v. Six Flags Entertainment Corporation*

Il caso *Rosenbach v. Six Flags Entertainment*[298] riguarda un celebre contenzioso emerso nel 2016, in relazione alla rilevazione dei dati biometrici di un minorenne dell'Illinois da parte del *Six Flags*, un popolare parco tematico statunitense. La vicenda legata al caso risaliva alla primavera del 2014, quando la signora Stacy Rosenbach aveva deciso di acquistare come regalo per suo figlio un abbonamento stagionale per il parco tematico, senza essere informata della contestuale rilevazione obbligatoria delle impronte digitali del figlio per poter ottenere l'accesso al parco tematico.

Infatti, sebbene fosse stata la madre a fornire liberamente i dati personali del figlio nel processo di iscrizione online, nessuna indicazione durante le fasi di iscrizione aveva informato la signora del fatto che per ottenere l'abbonamento fosse necessario disporre la registrazione delle impronte digitali del soggetto intestatario del biglietto. Pertanto, il figlio della signora Rosenbach, un ragazzino all'epoca dell'età di quattordici anni incapace di comprendere le implicazioni del trattamento al quale si stava sottoponendo, dopo essersi recato all'ingresso del parco fu sottoposto alla rilevazione delle sue impronte senza che avesse prestato il suo consenso e senza che gli fosse stata fornita alcuna informazione sulla natura del trattamento e sul modo in cui i suoi dati sarebbero stati conservati e impiegati dopo la scadenza del suo abbonamento. Inoltre, il parco tematico non aveva nemmeno specificato per quanto tempo avrebbe disposto la conservazione dei dati raccolti[299].

Dunque essendo i Rosenbach tutelati dalle previsioni dell'Illinois BIPA, ne emerse un contenzioso per ottenere un risarcimento per le violazioni in materia di informativa e consenso nella disposizione del trattamento dei dati biometrici da parte del parco. L'oggetto della contesa era verificare se il parco tematico avesse disposto correttamente la raccolta delle impronte digitali del minore ai sensi delle disposizioni dell'Illinois BIPA, avendole raccolte senza ottenere il consenso del minore e senza comunicare la natura del trattamento[300]. In particolare, l'obiettivo della corte era determinare se la parte lesa, in questo caso il minore, avesse effettivamente subito un danno piuttosto che un semplice effetto negativo dovuto alla violazione dei requisiti tecnici disposti per legge.

Nel giudicare se il ricorrente fosse stato effettivamente leso in un suo diritto, il giudice d'appello stabilì che il ricorrente dovesse addurre le prove di una lesione o un danno effettivo ai sensi del BIPA e non solo una mera violazione tecnica dei precetti della legge. Infatti nel determinare la natura della definizione di "parte lesa" ai sensi della legge BIPA la corte stabilì che l'intento del legislatore, nel

[298] Rosenbach v. Six Flags Entm't Corp. (Rosenbach l), No. 2-17-0317, 2017 WL 6523910, at *1,111. App. Ct. Dec. 21, 2017.

[299] E. M. Ghelardi, *Closing the Data Gap: Protection Biometric Information under the Biometric Information Privacy Act and the California Consumer Protection Act,* in *St. John's Law Review*, 94(3), 2020, p. 869-872.

[300] J. Swafford, *Rosenbach v. Six Flags Entertainment Corp.*, in *Federal Communications Law Journal*, 72(2), 2020, p. 297-299.

disporre del termine "leso", fosse volto a impedire che i singoli individui potessero avanzare pretese basate sulla mera violazione di legge[301]. Secondo le osservazioni della corte, la violazione tecnica riscontrata nell'assenza dei presupposti di informativa e consenso non configurava la definizione di parte lesa individuata nel BIPA. Pertanto, la corte concluse che per configurarsi come parte lesa l'individuo dovesse necessariamente addurre una prova concreta del danno subito dalla violazione tecnica della norma, stabilendo un'interpretazione delle disposizioni dell'Illinois BIPA decisamente più favorevole per alle imprese. Conseguentemente, non essendo riuscito a provare il danno subito, al ricorrente non venne attribuito il diritto al risarcimento del danno.

Tuttavia, agli inizi del 2019, la Corte Suprema d'appello dell'Illinois rigettò l'interpretazione della definizione di parte lesa adottata dalla Corte d'appello nel 2017, sovvertendo la sua sentenza[302]. Infatti, secondo la Corte Suprema l'aggettivo "leso" doveva essere interpretato nel suo significato ordinario come introdotto dal legislatore durante l'elaborazione della legge e pertanto, il suo significato non doveva essere ricondotto necessariamente a un danno economico o materiale subito dall'individuo. Infatti, secondo la Corte l'uso della tecnologia biometrica poteva definirsi ormai talmente pervasivo, da rappresentare autonomamente un rischio per la privacy degli individui già solo per semplici violazioni delle disposizioni di legge. Pertanto nel caso in questione, il ricorrente avrebbe avuto diritto al risarcimento anche senza addurre delle prove concrete del danno subito in relazione della violazione della propria privacy. Secondo le conclusioni della Corte Suprema, non è dunque necessario, ai sensi del BIPA, che un individuo alleghi un danno effettivo per qualificarsi come parte lesa e avere il diritto a chiedere il risarcimento del danno subito[303].

Pertanto, se la prima sentenza della Corte d'appello aveva introdotto un'interpretazione delle disposizioni della legge più favorevole alle imprese, limitando di fatto il numero delle azioni legali perseguibili dai ricorrenti, con la sentenza della Corte Suprema si afferma invece un'interpretazione volta ad anteporre la tutela dei singoli individui, obbligando le aziende private ad adottare ogni precauzione possibile per prevenire anche i ricorsi basati su mere violazioni di legge.

3.2 Il caso *Rivera v. Google Inc.*

Nello stesso anno del caso *Rosenbach*, emerse un altro contenzioso giudiziario legato all'interpretazione delle disposizioni dell'Illinois BIPA. Il caso in questione, denominato *Rivera v.*

[301] K. Singleton, *Illinois Appellate Court Holds That BIPA Plaintiffs Must Show Actual Harm*, in *JDSUPRA*, 28 marzo 2018. https://www.jdsupra.com/legalnews/illinois-appellate-court-holds-that-62705/
[302] See Rosenbachv. Six Flags Entm't Corp. (Rosenbach II), 129 N.E.3d 1197, 1204, 1207 Ill., 2019.
[303] C. Stepney, *Actual Harm Means It Is Too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law*, in *Layola of Los Angeles Entertainment Law Review*, 2019, 40(1), p.63-66.

Google Inc.[304], aveva ad oggetto l'applicazione di *Google Photos* e le rivendicazioni di una residente dell'Illinois, la quale denunciava come il software dell'applicazione avesse illecitamente sottoposto a scansione le sue foto personali, creando un modello digitale della geometria del suo volto senza che lei avesse acconsentito al trattamento dei suoi dati biometrici. La donna, infatti, nell'intraprendere un'azione legale contro Google rivendicava una grave violazione delle disposizioni dell'Illinois BIPA in termini di informativa e consenso dell'interessato, adducendo come il servizio di *photo tagging*[305] dell'azienda potesse determinare l'età, il genere e la localizzazione dell'individuo ritratto in foto senza informarne l'interessato[306]. Il servizio di *Google Photos*, di fatto, agisce creando una scansione del volto ritratto al momento del caricamento della foto, trasformandola in un modello digitale per etichettarlo e confrontarlo con le foto precedentemente salvate, per consentire al soggetto di individuare in modo semplice le foto analoghe ritraenti la medesima persona. Tuttavia, questo servizio veniva introdotto senza il consenso esplicito dell'interessato e senza specificarne la natura del trattamento, il tempo di conservazione dei dati e le modalità di eliminazione delle informazioni biometriche, ossia in assenza dei requisiti specifici introdotti dalla disciplina del BIPA e secondo la ricorrente la violazione si configurava ai sensi del BIPA in quanto al momento della scansione della foto il dispositivo aveva un indirizzo IP basato in Illinois[307].

Il Tribunale distrettuale del Distretto settentrionale dell'Illinois doveva dunque determinare se le informazioni derivate dalla scansione di una foto potessero configurarsi a tutti gli effetti come informazioni biometriche ai sensi del BIPA. Infatti, ai sensi della sezione §10 del BIPA le fotografie sono espressamente escluse dalla categoria di identificatori biometrici e poiché, secondo la definizione posta dalla legge le informazioni biometriche sono informazioni determinate esclusivamente dalla rilevazione di identificatori biometrici, le caratteristiche rilevate da una foto non dovrebbero configurarsi come dati biometrici. Invece, la Corte adottò un'interpretazione diversa delle disposizioni della sezione § 10 del BIPA[308] stabilendo che, poiché in tal caso il software di Google aveva applicato sistemi di rilevazione biometrica sulla foto per derivarne un modello della geometria facciale, il modello del volto derivato dalla scansione della foto costituiva a tutti gli effetti un identificatore biometrico. Dunque, nel caso in questione la manipolazione di un identificatore biometrico rilevato a partire da una fotografia configurava a tutti gli effetti un'informazione biometrica protetta dal BIPA, in quanto l'informazione rilevata dalla fotografia veniva impiegata per

[304] Rivera v. Google Inc. (Rivera 1), 238 F. Supp. 3d 1088, 1091, N.D. Ill., 2017.
[305] L'azione di "taggare" una foto significa etichettarne digitalmente le persone ritratte al suo interno, in modo da poterle successivamente identificare immediatamente.
[306] F. Q. Nguyen, *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, cit., p. 69.
[307] Vi sono ambiguità sul fatto che la disciplina del BIPA possa applicarsi altrimenti, se le scansioni del volto sono avvenute al di fuori dai territorio dello stato, anche se il caricamento della foto è avvenuto in Illinois.
[308] C. N. Insler, *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, in *Southern Illinois University Law Journal*, 2019, 43(4), p. 822-823.

indentificare in modo univoco l'individuo ritratto nella foto. La Corte, inoltre, respinse la difesa adottata da Google, secondo la quale solo le scansioni del volto effettuate in persona potevano configurarsi come identificatori biometrici ai sensi del BIPA[309]. Infatti, secondo la Corte non era rilevante come venisse raccolto l'identificatore, se in presenza o digitalmente, per configurarsi come identificatore biometrico. Nell'atto di scansionare la foto, l'applicazione di Google disponeva di fatto la trasformazione dei dati rilevati dalla foto in un modello biometrico del volto, che secondo la Corte poteva essere classificato unicamente come una scansione della geometria del volto del soggetto ritratto, che all'interno delle disposizioni del BIPA si configura espressamente come un identificatore biometrico, indipendentemente se il dato sia rilevato a partire da una persona fisica o da una fotografia. Pertanto, nel respingere l'argomentazione di Google, la Corte aveva adottato una nuova interpretazione delle disposizioni del BIPA, togliendo forza all'argomentazione dell'esclusione della fotografia dalla definizione di identificatore biometrico a titolo difensivo[310].

Nel caso in cui Google avesse semplicemente disposto l'archiviazione della foto senza eseguire una scansione biometrica della geometria del volto, non si sarebbe configurata nessuna violazione non essendo le foto ricomprese all'interno della definizione di identificatore biometrico. Di fatto, il contenzioso in *Rivera v. Google* ha ampliato la definizione di ciò che può essere classificato come identificatore biometrico, ricomprendendovi le scansioni del volto effettuate a partire da fotografie digitali. Tuttavia, nel Dicembre del 2018 in secondo grado di giudizio[311] Google ha ottenuto un giudizio sommario e la causa è stata respinta dalla Corte, in quanto in sede di giudizio i ricorrenti non avevano addotto delle prove sufficienti del danno subito in relazione alle violazioni in materia di informativa e consenso, nel trattamento degli identificatori biometrici[312]. Secondo la Corte nel caso in esame non sussisteva, pertanto, il rischio di una violazione e di una successiva diffusione illecita dei dati raccolti, sostenendo che i ricorrenti non potessero addure un danno concreto per stabilire una violazione perseguibile ai sensi della disciplina dell'Illinois BIPA.

[309] A. L. Metzger, *The Litigation Rollercoaster of BIPA: A comment on the Protection on Individuals from Violations of Biometric Information Privacy*, cit., p. 1068-1069.
[310] C. N. Insler, *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, cit., p. 822-823.
[311] Rivera v. Google Inc. (Rivera II), 366 F. Supp. 3d 998, 1006, N.D. Ill. 2018.
[312] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, cit., p. 250.

3.3 Il caso *In re Facebook*

Un altro caso simile a *Rivera v. Google Inc.* emerso negli stessi anni in relazione alla funzione di *tag suggestion*[313] di Facebook, noto come *In re Facebook*[314], ha contribuito ulteriormente a definire i contorni della disciplina dell'Illinois BIPA.

Nel caso in questione i ricorrenti rivendicavano come il sistema di *tag suggestion* adottato da Facebook agisse contrariamente alle disposizioni del BIPA, predisponendo la scansione del volto degli individui sulla base delle foto caricate per crearne dei modelli biometrici senza notificare il trattamento e raccogliere il consenso dei soggetti coinvolti[315]. Il modello di *tag suggestion* di Facebook dispone, infatti, un processo di riconoscimento facciale articolato in quattro fasi[316], di cui nella prima fase di rilevamento il software cerca di rilevare i volti a partire dalle foto postate e successivamente dispone la standardizzazione in termini di dimensioni e orientamento (fase di allineamento). Nelle fasi successive il software di Facebook elabora per ogni volto rilevato e allineato, una stringa di numeri identificativa per rappresentare l'immagine specifica di un volto (fase della rappresentazione), detta anche "firma del volto", mentre da ultimo le firme del volto vengono classificate all'interno di un database, che realizza corrispondenze fra i modelli dei volti rilevati e quelli precedentemente memorizzati (fase di classificazione).

Nel contenzioso questo sistema veniva contestato alla base in quanto non venivano adottati i presupposti in materia di informativa e consenso dell'interessato ai sensi del BIPA e inoltre, il colosso dei social mancava anche nel disporre la durata della conservazione dei dati e la natura del loro trattamento. In sua difesa dinanzi alla Corte, Facebook sostenne le argomentazioni alla base della prima sentenza nel caso *Rosenbach I*, adducendo che i ricorrenti non avessero adotto prove sufficientemente concrete del danno subito. Tuttavia, la Corte respinse l'argomentazione di Facebook sostenendo che l'interpretazione corretta delle disposizioni dell'Illionois BIPA fosse che la parte lesa si configuri in relazione alla violazione di un diritto legale tutelato dalla legge[317]. Dunque, l'interpretazione corretta delle argomentazioni emerse nel caso *Rosenbach (I & II)* stabiliva come fosse sufficiente la lesione di un diritto della privacy per configurare una violazione ai sensi della legge dell'Illinois.

---

[313] La funzione di *tag suggestion* è definita come un servizio volto a eseguire la scansione dei volti ritratti in foto per identificare i soggetti ivi raffigurati, promuovendo la codifica degli utenti. Dopo aver memorizzato le scansioni facciali dei soggetti ritratti, il software suggerisce i profili da poter *taggare* (etichettare) all'interno delle foto postate online.

[314] In re Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535, 540, N.D. Cal., 2018.

[315] R. Schwartz, *Patel V. Facebook, Inc: Biometric Data Collection Changes the Interpretation of Concrete Injury for Intangible Harms*, in *Tulane Journal of Technology and Intellectual Property*, 2020, 22, p. 263-264.

[316] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, cit., p. 251.

[317] J. Robles, *Patel v. Facebook, Inc.: the Collection, Storage, and Use of Biometric Data as a Concrete Injury under BIPA*, in *Golden Gate University Law Review*, 2020, 50(1), p. 67-68.

Il caso *In re Facebook* ha contribuito ad ampliare ulteriormente le tutele in materia di biometria, inizialmente ridotte nel primo caso *Rosenbach* del 2017, riducendo i presupposti necessari ai sensi del BIPA per poter adottare un'azione legale. Anche questa sentenza, infatti, ha esteso ulteriormente il numero dei contenziosi esperibili sotto la disciplina del BIPA a discapito delle aziende private. La sentenza ha di fatto determinato un notevole incremento nelle tutele a favore dei singoli individui, in quanto essendovi maggiori possibilità che un ricorrente abbia successo nell'intentare una causa legale per ottenere un risarcimento a fronte delle inadempienze di un ente privato, i privati saranno ulteriormente incentivati ad applicare rigorosamente la legge in materia di biometria[318].

3.4 Il caso *Monroy v. Shutterfly, Inc.*

In *Monroy v. Shutterfly*[319], il ricorrente Alejandro Monroy sosteneva che il sito web *Shutterfly*, dedicato alla realizzazione di prodotti personalizzati con le fotografie caricate dagli utenti, avesse trattato illegittimamente i suoi dati biometrici senza informarlo sulla natura del trattamento e verificarne il consenso[320]. Secondo il signor Monroy, infatti, la foto da lui caricata sul sito era stata indebitamente sottoposta a scansione per determinarne un modello della geometria del volto e identificarlo in ulteriori immagini senza il suo consenso. In sua difesa, invece, l'azienda sosteneva di aver semplicemente ricevuto la foto dal querelante e di aver rilevato i dati biometrici del soggetto estraendoli direttamente dalla foto. Pertanto, secondo l'azienda non poteva configurarsi una violazione ai sensi del BIPA in quanto la rilevazione della geometria del volto del soggetto non era avvenuta in presenza, ma a partire da una fotografia, la quale non costituiva un identificatore biometrico ai sensi del BIPA[321]. La Corte distrettuale ha rigettato la richiesta di archiviazione adottata da *Shutterfly*, non ritenendola un'interpretazione valida delle disposizioni della legge dell'Illinois, stabilendo che la rilevazione delle informazioni biometriche non debba necessariamente avvenire di persona[322]. Nella sua sentenza la Corte ha determinato come nel caso in questione il ricorso fosse legittimo, in quanto l'azienda aveva disposto la rilevazione della geometria del volto del soggetto ritratto in foto tramite l'utilizzo di sistemi di rilevazione biometrica. Inoltre, il ricorrente era riuscito a provare in modo sufficientemente ragionevole la natura del danno subito in relazione alle violazioni tecniche del trattamento.

---

[318] R. Schwartz, *Patel V. Facebook, Inc: Biometric Data Collection Changes the Interpretation of Concrete Injury for Intangible Harms*, cit., p. 271-272.
[319] *Monroy v, Shutterfly*, 16-CV-10984, 2017 WL 4099846, N.D. Ill. Sept. 15, 2017.
[320] C. N. Insler, *How to Tackle Litigation under the Biometric Information Privacy Act*, in *The Computer & Internet Lawyer*, 2018, 35 (12), 1-5, p. 2-3.
[321] B. Andra, *Facing the Facts on Biometric Phone Locks: Your Face and Thumb Are Not* Secure, in *University of Illinois Journal of Law, Technology &* Policy, 2018, 2, p. 421-422.
[322] F. Q. Nguyen, *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, cit., p. 70.

4. La necessità di incrementare lo standard statunitense per la protezione dei dati biometrici

Con l'aumento dei soggetti statunitensi pubblici e privati che introducono sistemi di rilevazione biometrica nei loro prodotti e servizi, si rivela sempre più essenziale l'adozione di una legge federale in materia di biometria, per introdurre un modello di regolazione uniforme in ogni stato. Nonostante vi sia chi sostenga che il *Federal Trade Commission Act* (FTC), il *Gramm-Leach-Bliley Act* (GLBA) e l'*Health Insurance Portability and Accountability Act* (HIPAA), costituiscano una disciplina sufficiente, nella realtà le loro disposizioni in materia di protezione di dati personali si rivelano insufficienti[323]. Infatti, questi atti legislativi rivolti alla regolazione dei trattamenti di dati personali e non dedicati in modo specifico alla disciplina biometrica, non offrono strumenti adeguati a regolare in modo dettagliato il trattamento di dati biometrici. In secondo luogo, abbiamo visto come in questo settore il principio di autoregolazione statale abbia portato solo pochi stati ad adottare una disciplina effettiva in materia di biometria, implementando leggi con modelli contrastanti, spesso incompatibili e lasciando la maggior parte dei territori statunitensi senza effettive tutele[324].

Se alcuni stati come l'Illinois, il Texas e Washington hanno riconosciuto l'importanza di una legislazione effettiva a tutela delle informazioni biometriche dei consumatori, l'insufficienza del modello di autoregolazione statale ci dimostra da tempo come sia giunto il momento di implementare un effettivo standard federale[325]. Fra questi infatti lo stato dell'Illinois, che con la legge BIPA ha adottato il modello di legislazione più avanzato in materia, è l'unico stato ad attribuire un effettivo potere ai singoli individui nel far valere le proprie rimostranze attraverso la possibilità di esperire ricorsi giudiziali. La sua portata tuttavia risulta limitata ai territori del suo stato e nonostante il BIPA rappresenti il modello più significativo per implementare una disciplina federale sui dati biometrici anche la sua applicazione non è stata sempre lineare, esponendo le aziende a un numero estremamente elevato di ricorsi[326], senza tutelare in ogni caso in modo adeguato i consumatori. Un modello che ha catalizzato in particolare l'attenzione dei giuristi statunitensi è il modello del GDPR europeo. Dalla sua implementazione nel 2016, infatti, il Regolamento generale sulla protezione dei dati ha catalizzato un forte dibattito in dottrina[327] volto a replicarne alcune disposizioni per incrementare le tutele in materia di privacy nell'ordinamento statunitense e adottare un unico modello di regolazione nella

[323] S. P. Mulligan, W. C. Freeman, C. D. Lineaugh, *Data Protection Law: An Overview*, in *Congressional Research Service*, 2019, p. 36-38.
[324] F. Q. Nguyen, *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, cit., p. 71-72.
[325] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, in *Journal of Law and Policy*, 2018, 26(2), p. 798-799.
[326] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* cit., p. 371-375.
[327] A. K. Rodrigues, E. R. Fedeles, M. E. Martin, *Existing and Emerging Biometric Data Technologies*, in A. Taal, *The GDPR Challenge: Privacy Technology and Compliance in an Age of Accelerating Change*, CRC Press, 2021, p. 163-168.

disciplina dei dati biometrici. L'attenzione degli americani per il GDPR europeo è data dal fatto che esso consente non solo di rafforzare le leggi sulla privacy nei territori europei, ma anche di rafforzare la tutela dei diritti dei cittadini europei rispetto alle imprese, enti e organizzazioni che vantano interessi economici in Europa. Come precedentemente analizzato, ai sensi dell'art. 9 il GDPR europeo classifica i dati biometrici come una categoria speciale di dati personali, attribuendogli tutele maggiori e una disciplina più estesa. Inoltre, il legislatore europeo tramite l'adozione del principio di *privacy by design* regolato all'art. 25 del GDPR, ha introdotto l'obbligo per le aziende di adottare delle forme di salvaguardia efficaci nell'uso di queste tecnologie fin dalle fasi iniziali del trattamento, misure del tutto assenti nella disciplina statunitense[328].

La forte asimmetria nei modelli europeo e statunitense pregiudica anche il lavoro di molte attività economiche americane, che si rivelano spesso troppo inadeguate nell'adottare gli standard di sicurezza necessari in materia di privacy per poter fare affari all'interno dell'Unione europea. Per questo da tempo nella dottrina statunitense si dibatte della possibilità di implementare un modello di regolazione federale in ambito biometrico basato sull'impianto del GDPR europeo, che ne imiti i presupposti essenziali senza incorrere nel rischio di ingessare troppo il mercato digitale statunitense[329]. In questa sezione analizzeremo in dettaglio le asimmetrie e i limiti delle leggi statali in materia di biometria discusse precedentemente, per determinare se sia possibile effettivamente ipotizzare un modello federale di regolazione dei dati biometrici e in che modo esso possa eventualmente emulare la disciplina di base posta dal GDPR europeo.

4.1 Le asimmetrie nelle leggi statali statunitensi in materia di biometria

L'Illinois, il Texas e Washington sono stati i principali promotori del movimento per l'adozione di una legislazione statale in materia di biometria. Tuttavia, le forti asimmetrie nei diversi modelli adottati in questi stati rendono sempre più difficile per le aziende adeguarsi alla loro disciplina per non incorrere in sanzioni[330]. Già solo le definizioni di identificatore biometrico o di informazione biometrica differiscono fortemente da uno stato all'altro, inoltre non tutti adottano una definizione specifica di informazione biometrica, focalizzandosi spesso esclusivamente sulla disciplina degli identificatori. A causa della mancanza di un'uniformità già solo nelle semplici definizioni di un identificatore o di un'informazione biometrica, le aziende possono risultare conformi alla disciplina di uno stato e incorrere in sanzioni in un altro, rendendo per quest'ultime estremamente difficile

[328] A. Romanou, *The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise*, in *Computer Law & Security Review 34*, 2018, 99-110, p. 104-105.
[329] F. Q. Nguyen, *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, cit., p. 77-81.
[330] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, cit., p. 259-260.

inserire nuovi prodotti sul mercato senza il rischio di essere sanzionate[331]. La legge dell'Illinois notoriamente attribuisce al soggetto la possibilità di esperire ricorsi giudiziali per far valere le proprie rimostranze e tutelare i propri diritti, anche se ciò ha avuto spesso esiti sfavorevoli per le aziende, senza implementare notevolmente le tutele dei consumatori. Invece, le leggi del Texas e di Washington non attribuiscono al soggetto la possibilità di ricorrere in giudizio per ottenere il risarcimento di danni provocati da violazioni dei loro statuti, ma attribuiscono al procuratore generale il compito di vigilare sulla corretta implementazione delle loro disposizioni[332].

Dato che nel secondo caso il procuratore generale è l'unico soggetto in grado di ricorrere in giudizio per le violazioni riscontrate da parte delle aziende è probabile che questo tipo di azioni legali non siano intraprese fino a che non si verifichi una violazione tangibile, riducendo le tutele dei consumatori e privandoli della possibilità di intraprendere ricorsi adeguati. Al contrario, sotto la tutela dell'Illinois BIPA, gli individui hanno spesso adottato dei ricorsi preventivi per mere violazioni di legge, quali l'assenza di un'informativa completa e della richiesta del consenso, prima che si verificasse una vera e propria violazione dei dati biometrici raccolti (quali una loro divulgazione non autorizzata o il loro utilizzo per scopi non consentiti)[333]. Per questo il modello della legge dell'Illinois viene generalmente privilegiato in quanto si ritiene che per la tutela del dato biometrico sia preferibile attribuire al privato la possibilità di esperire ricorsi giudiziali per ottenere un risarcimento, piuttosto che attendere che si configuri a tutti gli effetti una violazione nel trattamento di questi dati. Tuttavia, è necessario anche porre dei limiti specifici nel regolare queste tipologie di rimedi giudiziali per prevenire la possibilità di paralizzare il mercato digitale. Inoltre, ognuna di queste leggi adotta delle limitazioni specifiche sull'uso commerciale degli identificatori biometrici[334].

Anche in questo caso l'Illinois BIPA emerge come il modello più forte, predisponendo che un ente privato non possa raccogliere o rilevare un identificatore biometrico senza fornire preventivamente un'apposita informativa all'interessato e ottenerne il consenso al trattamento, rendendo obbligatorio per le imprese avere il consenso del consumatore anche se non stanno ancora rilevando alcun dato biometrico. Pure la legge del Texas impone alle aziende l'obbligo di ottenere il consenso prima di disporre la rilevazione dei dati biometrici, ma a dispetto del BIPA adotta una definizione diversa per gli indicatori e le informazioni biometriche, modificando leggermente il contenuto dell'informativa che deve essere notificata al consumatore prima di disporre il trattamento. La legge dello stato di

[331] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, cit., p. 789-793.
[332] B. Benson, *Fingerprints Not Recognized, Why the United States Needs to Protect Biometric Privacy*, in *North Carolina Journal of Law & Technology*, 2018, 19(4), p. 176-179.
[333] P. Smith, *BIPA: What Does It Stand for?*, in *Chicago Kent Law Review*, 2020, 95(3), p. 843-844.
[334] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* cit., p. 363-368.

Washington, invece, si discosta dalle precedenti esonerando le aziende dal fornire l'informativa e ottenere il consenso dell'interessato, nei casi in cui dispongano la semplice rilevazione dell'identificatore biometrico senza classificarlo successivamente[335]. Ciò agevola notevolmente le aziende che nei trattamenti che richiedono un'unica rilevazione possono procedere senza dover richiedere ogni volta il consenso dell'individuo, velocizzandone notevolmente l'acquisizione dei dati. Invece, risultano indebolite ulteriormente le tutele a favore dei singoli consumatori in quanto, se l'identificatore biometrico viene utilizzato solo per un tempo limitato e in seguito distrutto, le aziende generalmente adottano più superficialmente i protocolli di sicurezza[336].

Sebbene sia generalmente essenziale informare l'utente e ottenerne il consenso esplicito, in certi contesti effettivamente queste pratiche possono risultare superflue e costituire un onere burocratico sproporzionato per le aziende. Nel complesso possiamo determinare come l'Illinois BIPA sia la legge con la disciplina più estesa e severa in materia di protezione dei dati biometrici, mentre l'H.B. 1493 di Washington rappresenta il modello più flessibile e favorevole alle aziende. Oltre al confronto fra le singole leggi statali in materia di biometria, anche le singole interpretazioni giurisprudenziali delle disposizioni dell'Illinois BIPA si rivelano spesso confuse e inefficaci per le aziende. Le sentenze analizzate nel terzo paragrafo riguardano casi giudiziali determinanti nella giurisprudenza americana per discernere un livello di protezione adeguato nel tutelare la privacy biometrica di un individuo[337]. Se come nella sentenza *Rosenbach* II, la giurisprudenza interpreta una mera violazione tecnica dei presupposti stabiliti dalla legge come un danno effettivo meritevole di risarcimento, il consumatore ottiene garanzie notevolmente estese nella possibilità di ricevere un risarcimento per il danno subito[338]. Nella sentenza d'appello del 2019, la Corte Suprema dell'Illinois aveva infatti stabilito come anche una persona che avesse subito una violazione tecnica dei propri diritti e non un danno effettivo potesse essere titolata ad ottenere un risarcimento.

Pertanto, nella sentenza sul caso *Rosenbach II,* la Corte aveva aperto ai ricorrenti la possibilità di ricorrere in giudizio per ottenere un risarcimento, anche nei casi in cui l'azienda non avesse semplicemente fornito il giusto preavviso e richiesto il consenso. Anche se ciò comporta per le aziende maggiori attenzioni nel disporre le proprie politiche sulla privacy, non implica invece necessariamente un incremento nell'adozione di protocolli di sicurezza quando gli identificatori sono

[335] M. J. Anderson, J. Halpert, *Washington Becomes the Third State with a Biometric Privacy Law: Five Key Differences,* cit., p. 43-45.
[336] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* cit., p. 376-378.
[337] M. McMahon, *Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts,* in *Legal Studies Research Paper Series*, 2021, 65, p. 15-20.
[338] P. Smith, *BIPA: What Does It Stand for?*, cit., p. 847-850.

in loro possesso[339]. Più recentemente, anche il Tribunale distrettuale, intervenuto nella causa *In re Facebook* ha sostenuto che la lesione di un diritto sulla privacy sia sufficiente per configurare un danno ai sensi della disciplina del BIPA. Pertanto, a fronte di queste due sentenze attualmente nell'ordinamento dello stato dell'Illinois la violazione di legge configura a tutti gli effetti un danno risarcibile attraverso un ricorso giudiziale da parte del privato[340]. In netto contrasto, invece, la sentenza nel caso *Rivera v. Google Inc.* ha ridotto la capacità di far valere i propri diritti dei ricorrenti, in quanto la Corte ha ritenuto una violazione tecnica delle disposizioni del BIPA insufficiente per configurare un danno concreto. Nel caso in questione, l'applicazione *Google Photos* raccoglieva i dati biometrici della geometria del volto degli individui a partire da una fotografia. La decisione della Corte distrettuale non ha riconosciuto in questo caso l'intento legislativo alla base dell'emanazione del BIPA, in quanto l'esito della sentenza consentiva di fatto all'azienda di utilizzare l'assenza di un danno concreto a titolo difensivo[341]. I casi analizzati hanno anche concorso nell'ampliare la definizione di identificatori e informazioni biometriche per ricomprendervi le scansioni dei tratti facciali determinate a partire da una fotografia, anche se nelle disposizioni del BIPA le foto sono escluse dalle categorie di identificatori biometrici, rendendo ancora più difficile per le aziende determinare se siano o meno conformi alla legislazione in materia.

4.2 L'adozione di uno standard federale per la protezione dei dati biometrici

Attualmente negli Stati Uniti non esiste una legge federale per la tutela dei dati biometrici e gli unici interventi normativi in materia sono costituiti da leggi implementate da singoli stati, volte a regolare i trattamenti esclusivamente da un punto di vista commerciale[342]. Se però le leggi statali hanno una portata limitata, una disciplina federale sulla biometria attribuirebbe lo stesso livello di tutele ad ogni cittadino statunitense. L'approvazione di una legge federale sulla privacy biometrica concorrerebbe, infatti, a fissare una disciplina per queste pratiche commerciali uniforme in tutti gli stati, semplificando al contempo gli oneri burocratici a carico delle aziende che non dovrebbero più destreggiarsi fra leggi con disposizioni difformi ed eterogenee[343].

---

[339] M. McMahon, *Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts*, cit., p. 35-37.
[340] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* cit., p. 370-373.
[341] W. Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, in *Northeastern University School of Law*, 2021, 409, p. 101-103.
[342] D. L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, cit., p. 87.
[343] B. Benson, *Fingerprints Not Recognized, Why the United States Needs to Protect Biometric Privacy*, cit., p. 186-187.

In questa sezione ci concentreremo sull'analisi delle disposizioni che potrebbero orientare l'implementazione di una disciplina federale in materia di biometria all'interno dell'ordinamento statunitense. Di fatto, sulla base dei modelli fin qui analizzati è possibile definire in prima istanza alcuni criteri essenziali, quali l'individuazione di una definizione univoca per i concetti di identificatore biometrico e di informazione biometrica, la definizione dei limiti da apporre alla raccolta e all'archiviazione delle informazioni biometriche, la determinazione di se ed entro che limiti le aziende possano vendere o divulgare queste informazioni e, da ultimo, l'introduzione o meno di un diritto a ricorrere in giudizio per far fronte alle violazioni della propria privacy[344]. Inoltre, non dovrebbe essere sottovalutato nemmeno l'immenso potere di lobbying di cui godono le grandi aziende digitali statunitensi[345]. Queste aziende in passato hanno notevolmente condizionato i criteri adottati in alcuni stati, come la legge H. B. 1493 di Washington che di fatto ha un modello molto flessibile e favorevole alle imprese, contribuendo a bloccare l'adozione di iniziative legislative di questo tipo in altri stati. Per questo, se il Congresso decidesse di implementare una legge federale sulla privacy biometrica dovrebbe bilanciare attentamente le esigenze di sviluppo del mercato digitale con le tutele per i diritti dei consumatori, per non rischiare di soccombere alle prime.

Entrando nel merito di questi criteri di regolazione, per quanto concerne le definizioni sarebbe auspicabile adottare una definizione analoga a quelle contenute nelle leggi del Texas e dell'Illinois, applicando una distinzione fra identificatore biometrico e informazione biometrica[346]. In alternativa, il Congresso potrebbe adottare una definizione più espansiva del concetto di dato biometrico, atta a ricomprendere sia caratteristiche fisiche che comportamentali, come nella definizione del *Biometric Research Group*[347]. Inoltre, una legge federale in materia di biometria dovrebbe anzitutto risultare accorta e avveduta, per questo il Congresso oltre ad adottare una definizione esaustiva dovrebbe formulare una propria lista indicativa di identificatori biometrici tutelati dalla sua disciplina. In questo modo la legge tutelerebbe non solo le caratteristiche fisiche ma anche quelle comportamentali, mentre l'aggiunta di una lista non esaustiva di identificatori biometrici renderebbe la legge sufficientemente adatta a regolare sia le applicazioni attualmente esistenti, che gli sviluppi futuri delle tecnologie di identificazione biometrica. Infatti, questo settore in constante evoluzione preclude l'adozione di una lista realmente esaustiva, anche se estesa e integrabile nel tempo.

Dopo aver individuato una definizione inclusiva dei dati biometrici, è essenziale che il Congresso determini se adottare i requisiti di informativa e consenso per la raccolta di informazioni

[344] F. Q. Nguyen, *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, cit., p. 77.
[345] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, cit., p. 800-801.
[346] S. Roberg-Perez, *The Future in Now: Biometric Information and Data Privacy*, in *Antirtust*, 2017, 31(3), p. 61-63.
[347] Biometrics Research Group's definition of biometrics, Department of Computer Science and Engineering, Michigan State University. http://biometrics.cse.msu.edu/info/index.html

biometriche[348]. Per ridurre gli oneri burocratici a carico delle aziende potrebbe rivelarsi utile l'adozione a livello federale di un unico modulo di consenso al trattamento dei dati. Infatti, tramite la creazione di un unico modulo di consenso i cittadini sarebbero meno propensi a firmare alla cieca una loro autorizzazione, mentre le aziende sarebbero agevolate riducendo notevolmente i loro oneri burocratici. Al contempo, l'adozione di requisiti stringenti in termini di informativa e consenso obbligherebbero le aziende ad adottare standard di sicurezza più elevati nel trattamento di questi dati sensibili. Il Congresso dovrebbe inoltre stabilire i requisiti per la conservazione e la successiva eliminazione di questi dati[349]. Il requisito di conservazione meno restrittivo che il Congresso potrebbe adottare è quello che autorizza i soggetti commerciali a conservare i dati biometrici per "un tempo ragionevole", come disposto dalla legge di Washington, che integra ulteriormente queste disposizioni con tre ipotesi che giustifichino tempi di conservazione più lunghi.

Le leggi del Texas e dell'Illinois hanno invece adottato dei requisiti di conservazione leggermente più restrittivi indicando un termine specifico per l'eliminazione dei dati. Per trovare il giusto equilibrio tra la tutela della privacy e gli interessi commerciali delle imprese, si potrebbero adottare delle disposizioni federali a metà fra queste due tendenze, definendo un termine di conservazione specifico ma al contempo molto ampio[350]. Ad esempio, un termine di conservazione di tre anni potrebbe essere combinato con deroghe per le imprese, che per motivi eccezionali necessitino di termini di conservazione più lunghi. Il quarto elemento che il Congresso dovrebbe affrontare concerne la vendita e la divulgazione delle informazioni biometriche[351]. La legge dell'Illinois vieta espressamente la vendita delle informazioni biometriche raccolte, mentre ne autorizza la diffusione solo se richiesto da un'altra disposizione di legge.

Il modello del BIPA autorizza la divulgazione del dato anche nei casi in cui una società si trovi di fronte a una citazione in giudizio, un mandato o se necessaria per portare a termine una transazione finanziaria. Inoltre, per far sì che la diffusione del dato sia autorizzata in un qualsiasi contesto ai sensi del BIPA è necessario che l'individuo fornisca il suo consenso. Invece, le leggi del Texas e Washington consentono alle aziende di vendere e diffondere le informazioni biometriche nei casi in cui si configurino alcune eccezioni. La lista delle eccezioni del Texas è la medesima che autorizza la divulgazione dei dati ai sensi dell'Illinois BIPA, anche se in questo caso la medesima lista configura anche le eccezioni che autorizzano alla vendita dei dati. La lista delle eccezioni identificate dalla

[348] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation,* cit., p. 265-266.
[349] B. Benson, *Fingerprints Not Recognized, Why the United States Needs to Protect Biometric Privacy*, cit., p. 189-190.
[350] M. Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information,* cit., p. 398-404.
[351] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, cit., p. 797-802.

legge di Washington invece risulta ancora più ampia rispetto alle prime due. Per trovare un equilibrio anche in questo caso fra interessi privati e interessi aziendali, il Congresso potrebbe mediare fra le due posizioni adottando un modello simile a quello texano, dove la divulgazione e la vendita dei dati biometrici non sono del tutto vietate, ma sono consentite sono entro dei limiti stringenti accuratamente individuati per legge. Attribuire alle aziende la possibilità di vendere e divulgare informazioni biometriche in un numero limitato di circostanze tutelerà maggiormente la privacy degli interessati, senza soffocare le capacità operative di un'azienda.

L'ultimo elemento che il Congresso dovrebbe determinare riguarda la scelta dei possibili rimedi esperibili dal soggetto per tutelarsi rispetto a eventuali violazioni della propria privacy[352]. Come abbiamo visto la legge dell'Illinois è l'unica ad attribuire al soggetto la possibilità di ricorrere in giudizio per ottenere un risarcimento per i danni subiti. L'adozione di un simile sistema a livello federale da un lato incrementerebbe enormemente la tutela della privacy dei cittadini statunitensi, mentre dall'altro potrebbe sollevare numerose questioni legali e comportare un numero insostenibile di cause giudiziarie. Anche una stesura estremamente meticolosa non preverrebbe, infatti, la possibilità di numerose cause legali basate sull'interpretazione della legge. Tuttavia, una definizione chiara dei termini rilevanti e l'ideazione di un testo di legge completo e scrupoloso dovrebbero ridurre al minimo le possibilità di incorrere in contenziosi. Inoltre, l'attribuzione al privato della possibilità di esperire un ricorso attribuirebbe ai consumatori la possibilità di far valere i propri diritti senza dover dipendere dall'azione del procuratore generale.

L'esperienza legata ad altre leggi, come l'HIPAA, ha dimostrato come sottoporre le richieste di risarcimento a un ufficio governativo per la loro revisione non fornisca sempre lo stesso livello di protezione rispetto a una causa posta direttamente da un cittadino[353]. Dato che la compromissione di database biometrici potrebbe potenzialmente rovinare la vita di innumerevoli americani, casi che coinvolgano informazioni biometriche delicate non dovrebbero essere selettivamente perseguiti sulla base della discrezione di un piccolo gruppo di avvocati. Per questo un aumento del contenzioso derivante da cause poste direttamente dal cittadino costituirebbe un piccolo prezzo da pagare necessario per una più robusta protezione delle informazioni biometriche dei cittadini statunitensi. Il Congresso deve bilanciare la privacy e gli interessi commerciali per assicurarsi che una legge federale sulla privacy biometrica sia politicamente concretizzabile, ma non può piegarsi sotto la pressione del settore tecnologico ed escludere il diritto ad un ricorso privato per le sue violazioni[354]. L'insieme di queste semplici disposizioni tratte dall'analisi dei modelli delle leggi statali in materia di biometria

[352] I. T. Logan, *For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection*, in *Penn State Law Review*, 2019, 123(3), 779-812, p. 806-810.
[353] D. Cohen, *HIPAA Reform of a Patchwork Scheme: A Look at Preemption, Scope, and the Inclusion of a Private Right of Action in a New Federal Data Privacy Law*, in *American University Whasington College of Law*, 2020, p. 13-18.
[354] H. Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, cit., p. 643-648.

attualmente in vigore, potrebbero di fatto costituire una base concreta per guidare l'adozione di un'effettiva disciplina federale a in materia.

4.3 L'adozione dei principi del GDPR nella protezione dei dati biometrici negli Stati Uniti

La disciplina del Regolamento generale sulla protezione dei dati (GDPR) si estende sia alle organizzazioni interne all'Unione europea che alle organizzazioni collocate al di fuori dall'UE, che offrono beni e servizi al suo interno[355]. Infatti, pure le aziende statunitensi che dispongono dei dati personali di soggetti residenti nell'Unione europea, sono tenute a conformarsi alle sue disposizioni indipendentemente dalla loro ubicazione. Proprio per l'extraterritorialità delle sue previsioni e essendo ormai numerose le aziende americane soggette a questo tipo di regolazione per i loro interessi commerciali nei paesi europei, il GDPR ha catalizzato l'attenzione del legislatore statunitense. Da tempo di fatto si dibatte nella dottrina statunitense sulla possibilità di implementare un modello di regolazione federale per i trattamenti di dati sensibili basato sull'impianto del GDPR europeo, che ne imiti i presupposti essenziali senza incorrere nel rischio di ingessare troppo il mercato digitale[356]. Per porre un'analisi di queste tendenze come punto di partenza è necessario ripercorrere alcuni elementi decisivi introdotti dalla disciplina del Regolamento europeo.

In questo senso, le novità più importanti introdotte dal Regolamento includono: la sua applicabilità extraterritoriale; la disposizione di sanzioni specifiche; il consenso; la notifica della violazione dei dati; il diritto d'accesso; il diritto all'oblio; i principi della portabilità del dato e della *privacy by design* e l'obbligo per le aziende di indicare una figura responsabile del trattamento dei dati[357]. Ognuna di queste disposizioni si estende anche alle aziende extra-europee che effettuano trattamenti concernenti i dati di residenti europei. Inoltre, il GDPR introduce sanzioni proporzionali fino al 4% del fatturato globale annuo (o 20 milioni di euro) delle imprese non conformi ai suoi requisiti[358]. Il requisito europeo del consenso si rivela particolarmente elevato, in quanto prevede che la richiesta di consenso sia sottoposta in una forma facilmente accessibile e comprensibile, con allegato lo scopo del trattamento dei dati e la possibilità di ritirarlo in ogni momento[359]. Invece, per quanto concerne i diritti dell'interessato, il GDPR prevede un obbligo di notificazione al soggetto di ogni violazione dei

[355] M. Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information,* cit., p. 389-392.
[356] C. Llaneza, *An Analysis on Biometric Privacy Data Regulation: A Pivot towards Legislation Which Supports the Individual Consumer's Privacy Richts in Spite of Corporate Protections*, in *St. Thomas L. Rev.*, 2020, 32(2), p. 191-194.
[357] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation,* cit., p. 253-255.
[358] J. Trebble-Greening, *Rasing the Stakes: Creating an International Saction to Generate Corporate Compliance with Data Privacy Laws*, in *Columbia Business Law Review*, 2019, 2, p. 771-774.
[359] E. J. Kindt, *Having yes, using no? Abaout the new legal regime for biometric data*, cit., p. 537.

propri dati entro le 72 ore e i diritti di accesso, oblio e portabilità dei dati[360]. Inoltre, vi è sempre un diritto specifico ad essere informati sulla natura del trattamento dei propri dati, il luogo di conservazione e le finalità alla base della loro raccolta. Gli individui hanno anche diritto a una copia gratuita dei loro dati personali in formato elettronico e, se soddisfano le condizioni indicate dal regolamento, possono richiedere al responsabile del trattamento la cancellazione dei propri dati e di cessarne l'ulteriore diffusione nei confronti di terzi[361].

Il GDPR di fatto richiedere misure specifiche per il trattamento dei dati fin dalle prime fasi della loro acquisizione. I responsabili del trattamento sono tenuti ad adottare misure tecniche e organizzative sicure e a disporre l'elaborazione solo dei dati assolutamente necessari per il perseguimento delle finalità della raccolta, limitando invece l'accesso ai dati personali non strettamente necessari[362]. Inoltre, ai sensi del regolamento per alcune forme di trattamento viene richiesta anche la nomina di un responsabile della protezione dei dati[363], per rendere le procedure del regolamento meno burocratiche e più semplici da implementare, aumentando al contempo gli standard di sicurezza del trattamento. Ripercorrere le disposizioni generali alla base dell'impianto normativo del GDPR, fin qui brevemente riassunte, si rivela essenziale per potersi orientare nell'ipotesi di una loro adozione anche all'interno della disciplina sulla privacy statunitense, specialmente per quanto concerne il trattamento di dati biometrici. Se alcune di queste disposizioni concorressero ad orientare i legislatori statunitensi nell'adozione una disciplina federale sulla protezione dei dati biometrici, tendenzialmente si otterrebbe uno standard nazionale con livelli di sicurezza molto elevati e una disciplina decisamente più severa e articolata[364]. Molti accademici da tempo si interrogano sulla possibilità di implementare i principi europei all'interno dell'ordinamento statunitense. Lo scopo alla base di una simile riforma dovrebbe essere l'ideazione di uno standard nazionale per la regolazione dei trattamenti di dati biometrici che risulti uniforme in tutti gli stati, anche se un livello di regolazione così esteso potrebbe ottenere anche l'effetto indesiderato di ingessare eccessivamente il mercato digitale statunitense, con oneri burocratici troppo onerosi per le imprese[365].

Di seguito discuteremo le possibili implicazioni legate all'adozione di alcuni di questi principi. In primo luogo, l'adozione di sanzioni elevate come disposte nel GDPR avrebbe un forte potere dissuasivo nei confronti delle aziende, spingendole a conformarsi attentamente alle disposizioni per

[360] F. Q. Nguyen, *The Standard for Biometric Data Protection,* in *Journal of Law & Cyber Warfare*, cit., p. 79.
[361] J. Strycharz, J. Ausloos, N. Helberger, *Data Protection or Data Frustration? Individual Perceptions and Attitudes towards the GDPR,* in *European Data Protection Law Review (EDPL)*, 2020, 6(3), p. 410-411.
[362] M. Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information,* cit., p. 382-389.
[363] C. Llaneza, *An Analysis on Biometric Privacy Data Regulation: A Pivot towards Legislation Which Supports the Individual Consumer's Privacy Richts in Spite of Corporate Protections*, cit., p. 194-197.
[364] B. Benson, *Fingerprints Not Recognized, Why the United States Needs to Protect Biometric Privacy*, cit., p. 186.
[365] F. Q. Nguyen, *The Standard for Biometric Data Protection,* in *Journal of Law & Cyber Warfare*, cit., p. 81.

evitare ogni possibile sanzione[366]. Anche richiedere che il consenso sia prestato in una forma comprensibile e facilmente accessibile e che vi sia allegato lo scopo del trattamento, manterrebbe i consumatori statunitensi informati spingendo le aziende ad implementare queste forme di trattamento in modo responsabile. Inoltre, introdurre la possibilità di poter ritirare facilmente il proprio consenso al trattamento, agevolerebbe gli individui nel disporre di un controllo effettivo sui propri dati. I diritti individuali introdotti dal GDPR, invece, aumenterebbero il numero azioni esperibili nei ricorsi giudiziali per tutelare l'individuo rispetto alle violazioni subite, mentre il requisito che gli individui siano informati delle violazioni dei dati entro le settantadue ore, agevolerebbe gli individui permettendogli di reagire tempestivamente in caso di violazione dei dati[367].

Anche conoscere lo scopo e la natura del trattamento, nonché il luogo di conservazione dei dati permetterebbe agli interessati di verificare e correggere eventuali informazioni errate. Mentre la possibilità di ottenere una copia gratuita dei dati personali raccolti in formato elettronico consentirebbe agli individui di confrontarsi con l'insieme dei dati raccolti sul loro conto[368]. Così i consumatori sarebbero in grado di determinare chi ha accesso a tali informazioni e come intendono utilizzarle. Inoltre, fornendo un facile accesso a questi dati, gli individui acquisirebbero una maggiore consapevolezza delle informazioni condivise con le aziende. Ad esempio, in un caso di cronaca recente[369] che ha destato molto scalpore una cittadina europea aveva richiesto una copia delle informazioni raccolte sul suo conto al celebre sito di incontri americano *"Tinder"*, ottenendo sorprendentemente un report di centinaia di pagine contenente testimonianze di alcune delle sue confidenze più intime e private. In assenza di una regolazione specifica, queste informazioni sensibili potevano essere di fatto viste da molti impiegati dell'azienda o da chiunque comprasse le informazioni da essa. Dunque, l'aggregazione di questi dati legati ai nostri identificatori biometrici consente anche ad estrani di conoscere aspetti della nostra intimità, in alcuni casi addirittura con una visione più completa di quella che possiamo avere di noi stessi. Se persone del tutto estranee possono avere accesso a dettagli così intimi sulle vite delle persone, è giusto che ogni individuo abbia un accesso diretto al quadro completo dei suoi dati. Pertanto, attribuire agli individui il diritto ad ottenere i dati personali che li riguardino in un formato comunemente usato e leggibile a macchina, ne aumenterebbe il controllo sui loro dati sensibili[370]. L'implementazione della privacy by design del

[366] J. Trebble-Greening, *Rasing the Stakes: Creating an International Saction to Generate Corporate Compliance with Data Privacy Laws*, cit., p. 771-777.
[367] F. Q. Nguyen, *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, cit., p. 82.
[368] I. T. Logan, *For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection*, cit., p. 810.
[369] J. Duportail, *I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets*, in *The Guardian*, 26 settembre 2017.
https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold
[370] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* cit., p. 363.

GDPR modificherebbe il sistema attuale, invece, introducendo oneri specifici a carico delle aziende per la corretta messa in sicurezza dei dati all'interno di ogni fase della loro raccolta e successiva conservazione[371]. Le aziende dovrebbero così elaborare solo i dati strettamente necessari per il perseguimento dei loro scopi e limitare contestualmente l'accesso ai dati non necessari. In un contesto in cui la monetizzazione dei dati biometrici si sta sviluppando in tempi record, questo requisito si rivelerà cruciale per impedire alle aziende di raccogliere in massa questi dati unicamente per scopi di lucro, vendendo a terzi i dati biometrici dei consumatori[372]. Da ultimo, l'introduzione del requisito che prevede l'adozione di un responsabile del trattamento (*Data Protection Officer*)[373] da parte delle aziende non si rivelerebbe probabilmente un pesante fardello per il settore privato poiché il requisito si applicherebbe solo alle aziende con un ampio personale e che dispongono numerosi trattamenti di dati sensibili, mentre le aziende più grandi che elaborano dati biometrici a livello internazionale risulterebbero probabilmente già conformi a questo requisito, disponendo già da tempo ai sensi del GDPR l'elaborazione di dati di residenti dell'UE. L'applicazione dell'approccio del GDPR negli Stati Uniti consentirebbe pertanto ai consumatori di avere un maggiore controllo sulla raccolta, aggregazione e conservazione dei loro dati biometrici e di attribuire alle aziende oneri importanti quali la giustificazione della raccolta dei dati e la loro tutela in ogni fase del trattamento attraverso specifici requisiti di sicurezza.

5. Il trattamento di dati biometrici da parte di autorità pubbliche nell'ordinamento statunitense

Lo stato attuale della disciplina statunitense in materia di biometria si focalizza esclusivamente sui trattamenti di dati biometrici effettuati per scopi commerciali da imprese private. Di fatto, nell'ordinamento statunitense non esiste una definizione esplicita del concetto di trattamento di dati come nella disciplina europea e non si suddividono le forme di trattamento sulla base del loro ambito di applicazione come disposto nei precedenti capitoli[374]. L'ordinamento statunitense dispone esclusivamente una differenziazione sulla base dell'uso pubblico o privato di queste tipologie di dati sensibili, dove se i trattamenti di dati biometrici per scopi commerciali risultano almeno disciplinati in parte attraverso l'esperienza delle leggi nazionali adottate da vari stati, dal punto di vista di un uso

[371] A. Beduschi, *Rethinking digital identity for post-Covid-19 societies: Data Privacy and human rights considerations,* in *Cambridge University Press*, 2021, 3, 1-15, p. 5-6.
[372] L. Stewart, *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* cit., p. 357-360.
[373] C. Llaneza, *An Analysis on Biometric Privacy Data Regulation: A Pivot towards Legislation Which Supports the Individual Consumer's Privacy Richts in Spite of Corporate Protections*, cit., p. 194-197.
[374] K. A. Wong, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation,* cit., p. 232-235.

pubblico di questi dati da parte di organi e agenzie governative statali e federali si assiste, invece, alla totale assenza di ogni forma di regolazione. Eppure vi è un numero sempre più elevato di soggetti pubblici attivamente coinvolti nel trattamento di dati biometrici per finalità di prevenzione del crimine, sicurezza e contrasto al terrorismo, di cui possono disporre indiscriminatamente senza dover giustificare le loro finalità e senza dover incorrere in alcun tipo di limitazione[375].

Per questo l'assenza di una loro regolazione in mano pubblica ci pone di fronte a numerose questioni che di seguito analizzeremo in dettaglio. Nel primo paragrafo abbiamo visto come in realtà i cittadini statunitensi siano ben consapevoli della loro vulnerabilità a fronte di un uso pubblico indiscriminato di queste tecnologie, dati i loro forti poteri di controllo e ingerenza nelle vite individuali delle persone[376]. Da tempo, infatti, sono emersi numerosi movimenti politici e sociali che richiedono una regolazione effettiva dell'uso di questi sistemi da parte di soggetti pubblici, con l'attribuzione di forme di responsabilità concrete nei confronti dei cittadini danneggiati da un loro uso indebito. Ciò è avvenuto in parte, come già mostrato, attraverso l'adozione di specifiche leggi nazionali volte a vietare l'adozione di sistemi di riconoscimento facciale all'interno degli spazi pubblici[377]. Tuttavia, anche in questo caso queste normative si sono rivelate poco efficaci, in quanto in assenza di una disciplina federale che limiti l'uso di queste tecnologie da parte di organi governativi, questi soggetti pubblici non possono essere sottomessi alle disposizioni di semplici leggi statali che non hanno l'autorità per regolarne le competenze. Nello specifico il governo federale porta avanti iniziative di raccolta di dati biometrici da più tempo di quanto si possa ipotizzare. Ad esempio, l'FBI ha iniziato il suo programma nazionale di raccolta di impronte digitali già nel 1924 e nel 2007 ha fondato il *Biometric Center of Excellence*[378], che si occupa della supervisione e dell'implementazione dei sistemi nazionali di rilevazione biometrica. Inoltre, l'FBI si è occupata anche dello sviluppo del programma *Next Generation Identification* (NGI)[379], che consiste nel più grande ed efficiente archivio elettronico al mondo di informazioni biometriche e di storia criminale[380]. L'FBI non è però l'unica agenzia governativa che raccoglie dati biometrici, anche i Dipartimenti di Giustizia, Sicurezza Nazionale, Difesa e Stato, oltre ad altre numerose agenzie, lavorano assieme per raccogliere

[375] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, cit., p. 772-774.
[376] J. Andrew, M. Baker, *The General Data Protection Regulation in the Age of Surveillance Capitalism*, cit., p. 568-570.
[377] T. Simonite, *Face Recognition Is Being Banned – but It's Still Everyehere*, in *Wired*, 22 dicember 2021. https://www.wired.com/story/face-recognition-banned-but-everywhere/
[378] Il BCOE dell'FBI, con sede a Clarksburg, West Virginia, è il programma dell'FBI per esplorare e promuovere l'uso di tecnologie biometriche nelle loro operazioni. Ogni giorno, il BCOE si impegna a fornire strumenti e tecnologie biometriche all'avanguardia alle forze dell'ordine e al personale di intelligence che lavora nelle comunità di tutto il mondo. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence-1
[379] Il programma dell'FBI *Next Generation Identification* (NGI), costituisce il più grande ed efficiente archivio elettronico al mondo di informazioni biometriche e sulla storia criminale. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi
[380] J. Lynch, *Form Finger Prints to DNA, Biometric Data Collection in U. S. Immigrant Communities and Beyond*, in *Immigration Policy Center*, 2012, p. 10.

informazioni biometriche da inviare all'Ufficio di gestione dell'identità biometrica (*Office of Biometric Identity Management, OBIM*)[381], che ha sede nel Dipartimento di Sicurezza Nazionale. Oltre a queste agenzie federali, anche le forze dell'ordine statali, locali e tribali raccolgono e condividono dati biometrici con l'OBIM[382].

Gli attacchi dell'11 settembre 2001 hanno motivato gran parte di questa cooperazione fra diverse agenzie, così come la spinta per l'adozione di un programma nazionale relativo all'acquisizione di dati biometrici, rivolto specificamente a combattere il terrorismo[383]. L'OBIM sostiene di fatto come l'uso dei dati biometrici nella sicurezza nazionale per regolare gli accessi al paese, renda i sistemi di controllo talmente inviolabili da rendere praticamente impossibile accedervi per le cellule terroristiche. Uno dei primi grandi cambiamenti nella strategia biometrica nazionale è avvenuto nel 2003 quando il Dipartimento di Sicurezza Nazionale ha dato vita al programma "US-VISIT"[384]. Il programma US-VISIT è stato creato per tenere delle registrazioni accurate di tutte le persone che entrano ed escono dal paese, raccogliendo i dati biometrici dei visitatori, comprese le impronte digitali e le fotografie facciali ai valichi di frontiera e nei terminali degli aeroporti[385].

Come parte del vasto programma US-VISIT, tutti i richiedenti di un visto per gli Stati Uniti devono presentare i loro dati biometrici al Servizio Cittadinanza e Immigrazione degli Stati Uniti (USCIS) prima che le loro domande vengano elaborate, mentre successivamente il Dipartimento di Sicurezza Nazionale confronta questi dati con le liste dei terroristi certificati e altre liste di controllo per verificare l'identità degli individui. Il programma US-VISIT è stato usato anche per autorizzare la raccolta di dati biometrici appartenenti ai migranti che entrano illegalmente via mare e da altri territori di frontiera degli Stati Uniti[386]. Il Dipartimento di Sicurezza Nazionale sostiene che il programma US-VISIT abbia migliorato la sicurezza dei controlli alle frontiere in modo significativo, in quanto ha permesso alle forze dell'ordine di verificare l'identità di una persona prima di permetterle di entrare nel paese, rendendo i controlli più efficaci sia ai valichi di frontiera che negli aeroporti[387].

---

[381] L'Office of Biometric Identity Management fornisce servizi di corrispondenza biometrica, archiviazione, condivisione e analisi al DHS e ai partner di missione. La biometria supporta priorità fondamentali per la sicurezza nazionale, quali l'antiterrorismo e l'immigrazione. OBIM si concentra sulla fornitura di informazioni e analisi sull'identità biometriche accurate, tempestive e sicure. Gli obiettivi e le priorità generali di OBIM includono il continuo miglioramento dei servizi biometrici e l'accesso a dati biometrici ampliati per consentire le missioni operative del DHS.
Dal sito del Dipartimento di Sicurezza Nazionale: https://www.dhs.gov/obim

[382] N. Memon, *How Biometric Authentication Poses New Challenges to Our Security and Privacy*, cit., p. 196-197.

[383] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, cit., p. 775.

[384] Il programma US-VISIT del Dipartimento per la Sicurezza Nazionale degli Stati Uniti verifica in ingresso tramite l'uso della tecnologia biometrica l'identità di coloro che ottengono un visto per visitare il Paese.

[385] Homeland Security, *Enhancing Security Trough Biometric Identification*, US-VISIT program brochure. https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_biometrics_brochure_english.pdf

[386] S. Scheel, *Autonomy of Migration? Appropriating Mobility within Biometric Border Regimes*, Routledge, 2019, p. 42-51.

[387] J. J. Roberts, *Homeland Security Plans to Expand Fingerprint and Eye Scanning at Borders*, in *Fortune*, 12 settembre 2016. https://fortune.com/2016/09/12/border-security-biometrics/

Il governo sostiene, inoltre, che molti dei miglioramenti nell'immigrazione e nella sicurezza delle frontiere siano dovuti all'*Immigration and Customs Enforcement's* (ICE) *Secure Communities initiative*[388], un'iniziativa volta a migliorare l'interoperabilità tra le forze dell'ordine statali e locali e i database biometrici federali[389]. Questa interoperabilità permette alle forze dell'ordine locali di inviare i dati biometrici delle persone detenute sia all'FBI che al Dipartimento di Sicurezza Nazionale, per confrontare i loro dati biometrici con un database di immigrazione federale. Se i dati biometrici di una persona sono identificati nel sistema d'immigrazione come illegali, l'ICE può intraprendere un'azione esecutiva. Secondo i dati condivisi dall'agenzia, questa iniziativa ha portato negli anni alla rimozione di oltre trecentomila stranieri immigrati illegalmente negli Stati Uniti tra il 2008 e il 2014 e dal 2017 con la riattivazione del programma.

La cooperazione fra diverse agenzie ha anche portato alla creazione del Sistema Automatico di Identificazione Biometrica[390], noto come IDENT[391], che è sempre regolato dall'Ufficio di gestione dell'identità biometrica. Le statistiche sulla raccolta dati biometrici da parte di IDENT rivelano quanto siano diventate pervasive le rilevazioni governative. Di fatto, IDENT contiene attualmente oltre duecento milioni di identità biometriche ed elabora più di trecentomila transazioni biometriche al giorno. Una gran parte di queste transazioni proviene dalle forze dell'ordine statali e locali, che inviano circa cinquantamila campioni biometrici al giorno in tutto il paese. Queste cifre estremamente elevate dimostrano quanto siano estesi i programmi biometrici governativi statunitensi[392]. Il governo federale ha recentemente implementato anche diversi programmi pilota per la raccolta di dati biometrici negli aeroporti per i viaggiatori che lasciano gli Stati Uniti. Usando la tecnologia di riconoscimento facciale, i nuovi programmi di rilevazione in uscita confrontano dal vivo le scansioni facciali di un viaggiatore con la foto del loro passaporto per assicurarsi che corrispondano.

Tuttavia, il governo non rivela per quanto tempo i dati facciali potrebbero rimanere in suo possesso e poiché non vi è una regolamentazione specifica per queste tipologie di trattamento, non c'è garanzia che il governo distrugga effettivamente i dati biometrici o che lo faccia in modo tempestivo.

Il governo federale non è stato l'unico attore governativo ad aver aumentato la raccolta di dati biometrici dopo i fatti legati all'attentato dell'11 settembre. Anche diverse autorità statali hanno

---

[388] L'iniziativa Secure Communities mira a migliorare la sicurezza pubblica implementando un approccio completo e integrato per identificare e rimuovere i criminali stranieri dagli Stati Uniti. Il Secure Communities Program Management Office coordina tutte le attività di pianificazione operative, tecniche e fiscali dell'ICE dedicate alla trasformazione, alla modernizzazione e all'ottimizzazione del processo di rilevazione dei dati dei criminali.
Dal sito ufficiale dell'U.S. Immigration and Customs Enforcement (ICE): https://www.ice.gov/secure-communities

[389] J. Lynch, *Form Finger Prints to DNA, Biometric Data Collection in U. S. Immigrant Communities and Beyond*, cit., p. 6-9.

[390] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, cit., p. 777.

[391] Homeland Security, Office of Biometric Identity Management, *Biometrics*, https://www.dhs.gov/biometrics

[392] Homeland Security, *DHS/OBIM/PIA – Automated Biometric Identification System*, Privacy Impact Assessment https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf

adottato sistemi analoghi, come il governo della città di New York che ha creato un sistema di rilevazione biometrica noto come il *Domain Awareness System*[393]. Quest'ultimo è un programma antiterroristico sviluppato per facilitare l'osservazione delle attività preliminari delle organizzazioni terroristiche. Come parte del programma, la polizia di New York utilizza più di seimila telecamere in tutta la città attraverso una rete finanziata in parte dal Dipartimento per la Sicurezza Nazionale. Anche se il programma non utilizza direttamente un software di riconoscimento facciale, può raccogliere dati biometrici, come l'andatura di un individuo per garantire ad esempio il controllo del traffico pedonale[394]. Anche se il governo newyorkese cita molte ragioni legate alla sicurezza nazionale per giustificare la raccolta di questi dati biometrici, non dispone alcuna garanzia per i rischi significativi per la privacy di coloro che desiderino salvaguardare questi dati altamente sensibili[395].

È fondamentale notare anche come l'uso della biometria da parte delle forze dell'ordine ponga dei problemi specifici. Mentre può sembrare che la raccolta di dati biometrici da parte del governo possa interessare solo i viaggiatori, gli immigrati o coloro che vengono processati nel sistema della giustizia penale, molti americani che non hanno commesso alcun crimine sono sottoposti quotidianamente alla raccolta delle loro informazioni biometriche attraverso il programma NGI dell'FBI[396]. Inoltre, vi sono da tempo prove effettive della natura sproporzionata dei trattamenti effettuati dall'algoritmo del programma NGI nei confronti di minoranze afroamericane e latine[397]. Questo dato deve destare notevole preoccupazione in quanto dimostra come la tecnologia di riconoscimento facciale impiegata dall'FBI possa pregiudicare e identificare erroneamente queste categorie rispetto ad altri gruppi di persone. Inoltre, una recente modifica adottata per la disciplina del programma NGI stabilisce un'esenzione per l'FBI lasciando senza la possibilità di esperire un ricorso la maggior parte di coloro che vengono identificati erroneamente o che desiderano contestare in altro modo l'inclusione dei loro dati nel programma. Infatti, nel 2017, il programma è stato esentato dall'applicazione della disciplina del Privacy Act del 1974, citando ragioni di sicurezza nazionale[398]. Pertanto, l'FBI non dovrà più rivelare se i dati biometrici di un individuo siano inclusi nel database NGI e non avrà più bisogno del consenso per condividere i dati biometrici di un individuo con altre agenzie, e modificare il profilo

[393] Il Domain Awareness System è il più grande sistema di sorveglianza digitale al mondo nell'ambito della Lower Manhattan Security Initiative in collaborazione tra il Dipartimento di Polizia di New York e l'azienda Microsoft per implementare i sistemi di sicurezza di New York.
[394] E. S. Levine et al., *The New York City Police Department's Domani Awareness System*, in *Informs Journal on Applied Analytics*, 18 gennaio 2017. https://pubsonline.informs.org/doi/10.1287/inte.2016.0860
[395] Police Department, City of New York, *Domain Awareness system: Impact and Use Policy*, 11 Aprile 2021 https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/domain-awareness-system-das-nypd-impact-and-use-policy_4.9.21_final.pdf
[396] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, cit., p. 779.
[397] J. Lynch, *Form Finger Prints to DNA, Biometric Data Collection in U. S. Immigrant Communities and Beyond*, cit., p. 10.
[398] Z. Whittakaer, *FBI can keep secret who's in its biometrics 'mega database' says Justice Dept.,* in *ZDNet*, 8 agosto 2017. https://www.zdnet.com/article/fbi-to-keep-secret-biometrics-database-justice-department/

di un individuo nel programma. Molti esperti sostengono come questa esenzione abbia reso di fatto il Privacy Act privo di significato[399], lasciando i cittadini senza poter determinare se i loro profili biometrici contengano errori e senza la possibilità di ricorrere in giudizio. Questo sviluppo nella disciplina del database NGI ha già rilevato i propri limiti esponendo in più occasioni a un caro prezzo i soggetti identificati erroneamente attraverso il programma. Alcuni cittadini rispettosi della legge sono stati spesso identificati infatti erroneamente, come sospettati di terrorismo attraverso i programmi di identificazione biometrica del governo. Uno dei casi più celebri di queste inadempienze, ha coinvolto Brandon Mayfield[400], un avvocato e veterano dell'esercito dell'Oregon, che è stato erroneamente identificato come sospettato all'indomani degli attentati di Madrid del 2004. Dopo che un super computer dell'FBI ha abbinato erroneamente le impronte digitali di Mayfield con quelle trovate su una borsa sulla scena degli attentati, più analisti dell'FBI hanno erroneamente confermato la corrispondenza, nonostante altre quindici impronte digitali fossero state abbinate rispettivamente nel sistema. Come risultato, Mayfield fu soggetto alla confisca dei propri beni e sue proprietà e messo in prigione per oltre due settimane. Anche dopo che fu accertata la sua innocenza e come l'FBI avesse commesso un errore nell'identificarlo come sospettato, fu trattenuto come testimone materiale dell'attentato e i suoi movimenti continuarono ad essere dal governo. L'FBI alla fine fu tenuta a scusarsi con Mayfield, per la persecuzione ingiustificata alla quale l'aveva sottoposto, ma la sua storia resta comunque una testimonianza essenziale di come l'uso non regolamentato dei dati biometrici da parte del governo possa avere conseguenze disastrose per individui identificati erroneamente[401]. Senza una legislazione che protegga identità biometriche, non c'è nulla che possa fermare il ripetersi di casi futuri analoghi a questo.

[399] C. Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, cit., p. 780.
[400] S. M. Kassin, I. E. Dror, J. Kukucka, *The forensic confirmation bias: Problems, perspectives, and proposed solutions*, in *Journal of Applied Research in Memory and Cognition*, 2013, 2, p. 42-44.
[401] U.S. Department of Justice, *A Review of the FBI's Handling of the Brandon Mayfield Case*, Jenuary 2006. http://www.latent-prints.com/images/Final%20OIG%20Executive%20Summarylow.pdf

Conclusioni

Nella predisposizione di una disciplina in materia di biometria all'interno del contesto occidentale, l'ordinamento europeo e l'ordinamento statunitense adottano due approcci molto differenti. Nel primo abbiamo l'adozione del GDPR, un regolamento in grado di porre una disciplina sulla privacy molto avanzata ed estesa, mentre nel secondo abbiamo una concezione della tutela della privacy dei cittadini statunitensi molto diversa, connotata dall'assenza di qualsiasi forma di regolazione federale in materia di biometria volta a tutelare i diritti dei singoli individui.

Il contesto europeo emerge come un contesto più regolato, con uno dei modelli legislativi più efficaci per porre una tutela estensiva dei dati personali dei suoi cittadini, mentre in generale, negli Stati Uniti la disciplina sulla privacy si connota come un'area emergente del diritto statunitense che manca di una regolamentazione standardizzata a livello federale, che si riflette anche nell'ambito della regolazione dei sistemi di identificazione biometrica.

Nell'ordinamento europeo possiamo sintetizzare la disciplina sui dati biometrici attraverso un numero circoscritto di disposizioni, dall'art. 4, par. 14 GDPR che ne introduce una definizione univoca, agli artt. 6 e 9 GDPR che ne determinano le condizioni di liceità per il trattamento. Altre disposizioni del GDPR relative al trattamento dei dati sensibili riguardano le disposizioni generali relative al rispetto dei principi applicabili al trattamento dei dati; la previsione di sanzioni specifiche; il consenso; la notifica delle violazioni dei dati; il diritto di accesso; il diritto all'oblio; i principi di portabilità dei dati; privacy by design e l'obbligo per le aziende di designare un responsabile del trattamento.

Tuttavia, alcuni elementi tecnici essenziali come la raccolta, l'immagazzinamento e la conservazione di questi dati non sono affrontati in dettaglio e gli Stati membri sono lasciati soli nell'adottare regole nazionali aggiuntive, più severe e specifiche, che ad oggi si dimostrano le più urgenti per affrontare la regolamentazione del mercato relativa a queste tecnologie.

Inoltre, il trattamento di queste tecnologie algoritmiche proviene da contesti geografici significativamente diversi, il che complica ulteriormente la determinazione della giurisdizione competente per le controversie in materia. Anche nel caso di forme illegali di trattamento dei dati biometrici, è difficile determinare quale sia l'organo competente. Tutti questi elementi contribuiscono anche a livello europeo a rallentare l'aggiornamento della disciplina della responsabilità civile derivante dalle inefficienze di queste tecnologie per individuare il soggetto responsabile a cui attribuire gli eventuali danni. Questo complesso quadro giuridico nazionale e sovranazionale si rivela particolarmente oneroso per le aziende che utilizzano questi dati. Di qui, l'obiettivo di trovare un equilibrio tra la libera circolazione dei dati biometrici e la protezione dei cittadini non sembra ancora essere stato raggiunto. D'altro canto, nell'ordinamento statunitense si assiste ad un approccio

diametralmente opposto, che riflette una politica liberista volta a prediligere un approccio "*laissez fare*", piuttosto che un intervento mirato con una rigida disciplina sulla privacy che rischi di ingessare il mercato digitale. La tutela dei diritti del soggetto privato si determina prevalentemente in funzione della facilitazione di queste dinamiche di mercato, non prevedendo una regolazione federale sulla biometria e lasciando un ampio spazio di autonomia ai singoli stati.

I principali istituti sulla privacy attualmente in vigore sono le leggi federali del *Federal Trade Commission Act* (FTC), il *Gramm-Leach-Bliley Act* (GLBA) e l'*Health Insurance Portability and Accountability Act* (HIPAA). Nessuno di questi strumenti normativi dispone però una disciplina puntale sulla raccolta e l'utilizzo di dati biometrici; pertanto l'attuale quadro giuridico statunitense sull'identificazione e autenticazione di dati biometrici è caratterizzato esclusivamente dalla predisposizione di singole leggi statali. Infatti, nonostante il Congresso debba ancora emanare una regolazione federale, per quanto concerne la protezione e l'uso della biometria, alcuni stati quali il Texas, l'Illinois e Washington hanno già preso autonomamente una propria iniziativa sulla questione, guidando un movimento necessario. Attualmente negli Stati Uniti esistono unicamente tre leggi nazionali in materia di biometria promulgate dagli stati dell'Illinois, Texas e Washington, a cui deve essere aggiunta l'esperienza del *California Consumer Privacy Act* e di alcuni disegni di legge in corso di elaborazione in altri stati. Anche il *Commercial Facial Recognition Act* proposto nel 2019 da due senatori statunitensi, ha segnato un'esperienza significativa.

L'esperienza di queste leggi nazionali di fatto pone alcuni principi di base che possono orientare l'implementazione di una regolazione federale in materia, quali i requisiti di informativa e consenso per la raccolta di informazioni biometriche, i requisiti di conservazione e successiva eliminazione del dato, i requisiti per la vendita e la divulgazione di informazioni biometriche e la scelta dei possibili rimedi esperibili dal soggetto per tutelarsi rispetto alle violazioni della propria privacy. Ognuno di questi elementi viene regolato in modo autonomo all'interno della legislazione dei tre stati fin qui analizzati, tanto che le forti asimmetrie nei diversi modelli adottati rendono sempre più difficile per le aziende adeguarsi alla loro disciplina per non incorrere in sanzioni. Già solo le definizioni di identificatore biometrico o di informazione biometrica differiscono fortemente da uno stato all'altro; inoltre, non tutti adottano una definizione specifica di informazione biometrica, focalizzandosi spesso esclusivamente sulla disciplina degli identificatori.

A causa della mancanza di un'uniformità già solo nelle semplici definizioni di un identificatore o di un'informazione biometrica, le aziende possono risultare conformi alla disciplina di uno stato e incorrere in sanzioni in un altro, rendendo per quest'ultime estremamente difficile inserire nuovi prodotti sul mercato senza il rischio di essere sanzionate. Fra questi infatti lo stato dell'Illinois, che con la legge BIPA ha adottato il modello di legislazione più avanzato in materia, è l'unico stato ad

attribuire un effettivo potere ai singoli individui attribuendogli la possibilità di esperire ricorsi giudiziali. La sua portata, tuttavia, risulta limitata ai territori del suo stato e nonostante il BIPA rappresenti il modello più significativo per implementare una disciplina federale sui dati biometrici anche la sua applicazione non è risultata sempre lineare, come abbiamo visto nelle sentenze analizzate, esponendo le aziende a un numero estremamente elevato di ricorsi, senza tutelare in ogni caso in modo adeguato i consumatori.

Un modello che ha catalizzato in particolare l'attenzione dei giuristi statunitensi è proprio il modello del GDPR europeo. Dalla sua implementazione nel 2016, infatti, il Regolamento generale sulla protezione dei dati ha orientato un forte dibattito nella dottrina statunitense volto a replicarne alcune disposizioni per incrementare le tutele in materia di privacy nell'ordinamento statunitense e adottare un unico modello di regolazione nella disciplina dei dati biometrici. L'attenzione degli americani per il GDPR europeo è data dal fatto che esso non solo concorre nel rafforzare le leggi sulla privacy nei territori europei, ma consolida anche la protezione dei diritti dei cittadini europei rispetto alle imprese, enti e organizzazioni straniere che vantano interessi economici in Europa.

La forte asimmetria nei modelli europeo e statunitense pregiudica anche il lavoro di molte attività economiche americane, che si rivelano spesso troppo inadeguate nell'adottare gli standard di sicurezza necessari in materia di privacy per poter fare affari all'interno dell'Unione europea. Questa situazione è stata aggravata ulteriormente anche dall'adozione della Sentenza Schrems II, che ha invalidato la decisione di adeguatezza della legge statunitense del Privacy Shield, adottata nel 2016 dalla Commissione europea dopo la decadenza dell'accordo Safe Harbor, in quanto la Corte di Giustizia dell'Unione europea ha rilevato la non conformità rispetto alle disposizioni europee dei trattamenti svolti dagli Stati Uniti, ad eccezione che ad essi siano applicate le garanzie ulteriori previste nel GDPR o clausole contrattuali standard (CSS). Per questo da tempo nella dottrina statunitense si dibatte della possibilità di implementare un modello di regolazione federale in ambito biometrico basato sull'impianto del GDPR europeo, che ne imiti i presupposti essenziali senza incorrere nel rischio di ingessare troppo il mercato digitale statunitense.

Lo scopo alla base di una simile riforma dovrebbe essere l'ideazione di uno standard nazionale per la regolazione dei trattamenti di dati biometrici uniforme in tutti gli stati, anche se un livello di regolazione così esteso potrebbe ottenere anche l'effetto indesiderato di ingessare eccessivamente il mercato digitale statunitense, con oneri burocratici troppo gravosi per le aziende. Sia l'adozione di sanzioni elevate come disposte nel GDPR che l'adozione di un requisito sul consenso così esteso avrebbero un forte potere dissuasivo nei confronti delle aziende, spingendole a conformarsi attentamente alle disposizioni per evitare ogni possibile contenzioso. Inoltre, introdurre la possibilità di poter ritirare facilmente il proprio consenso al trattamento, agevolerebbe gli individui nel disporre

di un controllo effettivo sui propri dati. Anche conoscere lo scopo e la natura del trattamento, nonché il luogo di conservazione dei dati permetterebbe agli interessati di verificare e correggere eventuali informazioni errate, mentre la possibilità di ottenere una copia gratuita dei dati personali raccolti in formato elettronico consentirebbe agli individui di confrontarsi con l'insieme dei dati raccolti sul loro conto. Così i consumatori sarebbero in grado di determinare chi ha accesso a tali informazioni e come intendono utilizzarle. L'implementazione del principio della *privacy by design*, invece, introdurrebbe oneri specifici a carico delle aziende per la corretta messa in sicurezza dei dati all'interno di ogni fase della loro raccolta e successiva conservazione. Le aziende dovrebbero così elaborare solo i dati strettamente necessari per il perseguimento dei loro scopi e limitare contestualmente l'accesso ai dati non necessari. In un contesto in cui la monetizzazione dei dati biometrici non fa che svilupparsi a perdita d'occhio, questo requisito si rivelerà cruciale per impedire alle aziende di raccogliere in massa questi dati per scopi di lucro, vendendo a terzi i dati biometrici dei consumatori.

Da ultimo, l'introduzione del requisito che prevede l'adozione di un responsabile del trattamento da parte delle aziende non si rivelerebbe oneroso per il settore privato poiché il requisito si applicherebbe solo alle aziende con un ampio personale e che dispongono numerosi trattamenti di dati sensibili, mentre le aziende più grandi che elaborano dati biometrici a livello internazionale risulterebbero probabilmente già conformi a questo requisito, disponendo già da tempo ai sensi del GDPR l'elaborazione di dati di residenti dell'UE.

L'applicazione dell'approccio del GDPR negli Stati Uniti consentirebbe pertanto ai consumatori di avere un maggiore controllo sulla raccolta, aggregazione e conservazione dei loro dati biometrici e di attribuire alle aziende oneri importanti quali la giustificazione della raccolta dei dati e la loro tutela in ogni fase del trattamento attraverso specifici requisiti di sicurezza. Pertanto, ponendo un confronto effettivo fra l'ordinamento europeo e l'ordinamento statunitense, per quanto le disposizioni europee pongano una disciplina del dato biometrico più estesa e efficace, in grado di tutelare in modo più incisivo i diritti e le libertà dei cittadini europei, il modello statunitense detiene comunque alcuni elementi di pregio. Da un lato infatti esso è più attento alle pratiche di mercato, ponendo misure specifiche rivolte esclusivamente alla regolazione dei trattamenti di dati biometrici in ambito commerciale, mentre all'interno del GDPR non vi è un'attenzione specifica per la dimensione commerciale del mercato di questi sistemi biometrici, che invece rappresentano la maggior parte di trattamenti disposti nell'ambito della raccolta di queste tipologie di dati.

Dal punto di vista, invece, della regolazione dei trattamenti di dati biometrici da parte di autorità di pubblica sicurezza, se negli Stati Uniti si assiste a una fortissima deregolamentazione di questi sistemi, attribuendo un potere arbitrario estremamente ampio ad agenzie e organi federali e nazionali, in ambito europeo anche l'uso dei sistemi biometrici da parte dei poteri pubblici viene soggetto a

regolazione. Nell'Unione Europea l'adozione del regolamento generale sulla protezione dei dati (UE) 2016/679 è stata accompagnata dalla previsione di una direttiva che predisponesse delle misure chiare per la tutela delle persone fisiche in riferimento al trattamento di dati personali da parte di autorità pubbliche, per fini di prevenzione, indagine e perseguimento di reati.

In presenza di un quadro giuridico chiaro ed un uso proporzionato di questi sistemi, si è sempre ritenuto fondamentale garantire alle autorità di polizia l'accesso a queste tecnologie in funzione della tutela della pubblica sicurezza.

L'accesso a immagini facciali, impronte digitali o altri dati biometrici, se configurato all'interno di un'esigenza di interesse pubblico si può ritenere un'ingerenza necessaria nella vita delle persone per consentire di individuare e perseguire crimini, identificare sospetti e agevolare indagini giudiziarie. Attualmente, agenzie europee quali l'Eurodac e L'Europol dispongono quotidianamente la raccolta di dati biometrici di cittadini europei e non solo, all'interno di politiche di sicurezza in materia di immigrazione clandestina o per la creazione di una banca dati biometrica comune a livello europeo fra le varie forze di polizia nazionali. Anche se questi dati non sono necessariamente impiegati in funzioni di controllo una volta acquisiti, la loro raccolta e conservazione può costituire un'interferenza sproporzionata con il diritto alla vita privata delle persone, tanto più se sottoposti a forme di trattamento automatizzate e conservati in database di polizia. Per questo spetta pertanto al diritto nazionale dei singoli Stati membri regolamentare dettagliatamente la registrazione e la conservazione di questi dati per scopi di identificazione biometrica da parte di autorità pubbliche. Ad oggi una regolamentazione accurata sulla conservazione dei dati biometrici risulta ancora prevalentemente assente nel diritto nazionale degli Stati europei, nonostante l'esponenziale aumento della creazione di queste banche dati ed il rischio crescente di una loro raccolta senza una chiara base legale. Lo stato attuale della disciplina statunitense in materia di biometria, invece, si focalizza esclusivamente sui trattamenti di dati biometrici effettuati per scopi commerciali da imprese private. Di fatto, nell'ordinamento statunitense non esiste una definizione esplicita del concetto di trattamento di dati come nella disciplina europea e non si suddividono le forme di trattamento sulla base del loro ambito di applicazione come disposto nei precedenti capitoli.

L'ordinamento statunitense dispone esclusivamente una differenziazione sulla base dell'uso pubblico o privato di queste tipologie di dati sensibili, dove se i trattamenti di dati biometrici per scopi commerciali risultano almeno disciplinati in parte attraverso l'esperienza delle leggi nazionali adottate da vari stati, dal punto di vista di un uso pubblico di questi dati da parte di organi e agenzie governative statali e federali si assiste, invece, alla totale assenza di ogni forma di regolazione. Eppure vi è un numero sempre più elevato di soggetti pubblici attivamente coinvolti nel trattamento di dati biometrici per finalità di prevenzione del crimine, sicurezza e contrasto al terrorismo, di cui possono

disporre indiscriminatamente senza dover giustificare le loro finalità e senza dover incorrere in alcun tipo di limitazione. Nello specifico il governo federale porta avanti iniziative di raccolta di dati biometrici da più tempo di quanto si possa ipotizzare, ad esempio, attraverso il programma NGI e il *Biometric Center of Excellence* fondati dall'FBI, le attività dell'Ufficio di gestione dell'identità biometrica (OBIM) presso il Dipartimento per la Sicurezza Nazionale del Governo federale, il programma US-VISIT per monitorare gli accessi al paese, la *Secure Communities initiative* dell'ICE e il Sistema Automatico di identificazione biometrica IDENT.

L'assenza di un sistema di regole chiare nell'adozione dei sistemi di riconoscimento biometrico si rivela assai controversa. Infatti queste tecnologie predittive possono interferire notevolmente nella tutela della privacy delle persone coinvolte, mettendo in atto vere e proprie azioni di controllo e profilazione. Da un lato, lo sviluppo di queste tecnologie consente l'adozione di sistemi di sicurezza estremamente efficaci per la prevenzione del crimine e il contrasto al terrorismo. Dall'altro lato, dove non vi sono limiti chiari nel regolare l'uso di questi sistemi da parte del potere pubblico, vi è il rischio che questo potere possa rivelarsi arbitrario e tradire le sue finalità originarie di sicurezza e interesse pubblico. Non bisogna al contempo dimenticare come lo sviluppo di queste tecnologie sia guidato prevalentemente dagli investimenti di grandi aziende digitali, le quali costituiscono alcuni dei pochi soggetti in grado di investire il capitale economico necessario a finanziare la ricerca in questo campo, mentre il settore pubblico dipende fortemente da questi attori privati per avervi accesso. Pertanto, se può ritenersi controversa l'affermazione di un monopolio privato sullo sviluppo di queste tecnologie, un loro utilizzo indiscriminato da parte dei pubblici poteri al di fuori di un sistema di regole chiaro, può rappresentare rischi maggiori per i diritti e le libertà dei cittadini. Per questo analogamente al caso europeo con la risoluzione adottata il 6 ottobre 2021, anche negli Stati Uniti recentemente si è aperta una discussione sull'eventualità di apporre un vero e proprio divieto sull'uso del riconoscimento facciale all'interno degli spazi pubblici da parte di autorità di pubblica sicurezza culminato in una serie di provvedimenti nazionali volti a limitare l'impiego di tecnologie di riconoscimento facciale da parte delle autorità locali.

Pertanto, nonostante l'approccio europeo e statunitense differiscano notevolmente nella predisposizione di un modello di regolazione dei sistemi di riconoscimento biometrico, a fronte di un mercato digitale sempre più globale risultano strettamente interrelati. Per questo risulta fortemente auspicabile l'introduzione nella disciplina statunitense di alcuni istituti in materia della privacy disposti della disciplina europea, anche alla luce dei rinnovati ostacoli disposti dalla sentenza Schrems II in base alla quale attualmente le leggi statunitensi non garantiscono un livello di protezione adeguato ai sensi delle disposizioni del GDPR. Inoltre, anche la recente pubblicazione della proposta di Regolamento sull'approccio europeo all'Intelligenza Artificiale porrà sfide ulteriori alla

commercializzazione di questi sistemi tra mercato europeo e marcato statunitense. Essa, infatti, nonostante debba essere ancora approvata, pone le basi per un vero e proprio piano di modernizzazione della disciplina europea in campo biometrico, focalizzandosi in particolare sull'uso a fini identificatori di questi sistemi. L'approccio così codificato dal legislatore europeo sembra configurarsi come più votato ad uso etico di queste tecnologie ormai imprescindibili nel nostro quotidiano. Inoltre, all'interno questo mosaico giuridico, di cui tale regolamento costituirà l'ultimo tassello si cercherà non solo di favorire le opportunità che l'IA offre per le istituzioni, ma anche di valutarne approfonditamente i rischi e le responsabilità che i fornitori di beni e servizi dovranno assumersi all'interno di questo settore, andando probabilmente a incrementare ulteriormente i requisiti necessari per il trattamento di questi dati all'interno di banche dati estere.

Da ultimo, anche l'analisi della disciplina in materia di dati biometrici all'interno dell'ordinamento italiano si è rivelata essenziale per mettere a fuoco le strategie adottate dal nostro paese nel recepimento delle disposizioni europee in materia di biometria e nell'introduzione di una vera e propria disciplina nazionale più estesa rispetto a quella europea. Nel complesso di questo quadro giuridico nazionale e sovranazionale, con l'adozione delle disposizioni di garanzia sancite all'articolo 7 del Codice Privacy, anche l'Italia avrà la possibilità di adottare un proprio modello di regolazione dei sistemi di riconoscimento biometrici, incidendo sulle strategie di policy-making adottate a livello europeo.

Riassunto

L’avvento dell’uso della biometria e delle tecnologie ad essa connessa, ha accompagnato nuove riflessioni sul nostro concetto di identità e sulle libertà dei nostri corpi. Nonostante vi siano testimonianze storiche risalenti in merito all’adozione di forme di riconoscimento fondate su dati biometrici, è solo a partire dall’ultimo secolo e ancora maggiormente in quello attuale, che grazie al progresso tecnologico l’utilizzo di questa nuova forma di determinazione dell’identità ha conosciuto la sua massima espansione, trovando numerosi ambiti di applicazione e una grande varietà di scopi. Alla base del successo delle tecniche di riconoscimento biometrico e del loro impiego in larga scala vi sono l’unicità, l’universalità, nonché la facile “catturabilità” e la permanenza di questa tipologia di dati, tali da far sì che i nostri corpi si siano trasformati in delle vere e proprie chiavi di accesso, delle *password* di riconoscimento. Per tracciare l'evoluzione della disciplina dei dati biometrici nell’ordinamento europeo e statunitense, è necessario sottolineare la sua stretta interdipendenza con la disciplina sulla tutela della privacy. Se, da un lato, l'adozione di tecnologie basate sulla biometria viene spesso incoraggiata per migliorare la sicurezza dei sistemi informatici, in quanto considerate tecnologie di miglioramento della privacy (PET), dall'altro, il loro utilizzo e i margini di errore ad esse connessi possono avere conseguenze molto impattanti sulla vita dell'individuo. Dunque, i sistemi biometrici hanno campi di sviluppo e applicazione ampi e variegati. Il loro enorme potenziale ha attirato gli investimenti di privati e grandi aziende, che hanno utilizzato i dati biometrici per garantire l'accesso ai servizi, l'attivazione di dispositivi elettronici e sfruttare sistemi di Intelligenza Artificiale e Machine Learning, sebbene anche all'interno del settore pubblico, queste tecnologie stanno giocando un ruolo sempre più importante. Attualmente, il riconoscimento biometrico è utilizzato in misure per migliorare la sicurezza pubblica o nazionale, facilitare lo sviluppo di indagini criminali, combattere il crimine organizzato, garantire il controllo delle frontiere e scopi antiterroristici, e implementare l'efficienza di molti servizi pubblici. Tuttavia, la commercializzazione di questi sistemi di determinazione biometrica all'interno di diversi settori può rivelarsi altamente insidiosa e comportare molti rischi legati allo sfruttamento di questi sistemi, specialmente per quanto concerne il rispetto dei diritti e delle libertà fondamentali dei suoi utenti. Inoltre, la ricerca nello sviluppo di questo settore viene condotta prevalentemente da attori privati, giganti digitali, che detengono il capitale economico necessario per commercializzare questi sistemi nel mercato globale. Queste multinazionali detengono ormai un patrimonio di conoscenze su questi sistemi irraggiungibili per le autorità pubbliche. Queste ultime infatti hanno avuto solo un approccio tardivo alla biometria, riconoscendo i rischi di questi sistemi solo quando la loro diffusione era già ben avviata e difficile da limitare. Di fronte a una domanda di mercato in rapida crescita e al vuoto normativo prodotto

dall'indecisione legislativa, questi attori economici devono generalmente assumere un ruolo decisionale, tracciando i propri limiti. Tali attori privati, assumendo un ruolo semi-pubblicistico, agiscono spesso come intermediari necessari per la predisposizione di misure adeguate a proteggere i diritti fondamentali minacciati dall'uso di questi sistemi. Ad esempio, alcune multinazionali, come IBM, hanno deciso di sospendere il commercio di specifici sistemi di identificazione biometrica a causa delle troppe interferenze con il diritto alla privacy e delle forme di discriminazione determinate dalle imperfezioni algoritmiche alla base del loro funzionamento. Abbiamo quindi un contesto ibrido all'interno del quale questi soggetti privati determinano come e a quali condizioni consentire il commercio di queste tecnologie. Inoltre, il settore pubblico, che sta aumentando l'uso della biometria nella sicurezza pubblica e nella lotta al terrorismo, deve necessariamente affidarsi a operatori privati, spesso provenienti da potenze straniere, quali la Cina. Anche l'avvento della pandemia globale di Covid-19 ha portato a un crescente utilizzo di sistemi biometrici da parte di enti pubblici per misurare la temperatura corporea, rilevare volti senza maschere in spazi pubblici e tracciare i contagi, mostrando come governi e aziende si stiano rivolgendo a nuovi usi delle tecnologie biometriche per limitare il contagio e sviluppare opportunità economiche. Gli operatori economici che detengono il commercio di questi sistemi in termini monopolistici sono anche in possesso di una risorsa cognitiva senza precedenti, a seguito dello sviluppo di tecnologie in grado di raccogliere passivamente dati che, combinati con sistemi di analisi dei dati, possono determinare informazioni altamente accurate sulle abitudini, sui movimenti e sull'identità degli utenti interessati. Non è un caso che la professoressa di Harvard Shoshana Zuboff, analizzando la genesi di questi sistemi, abbia definito i dati biometrici come la nuova moneta dell'economia digitale, arrivando a teorizzare la nascita di un naturale "capitalismo della sorveglianza", dimostrando come i modelli di business adottati dai giganti digitali (come Facebook, Amazon e Google) generino nuove forme di accumulazione capitalistica digitale. È necessario evidenziare come il ruolo monopolistico svolto da queste multinazionali nel mercato digitale assuma anche una valenza politica primaria poiché questi soggetti determinano le condizioni per il commercio di questi sistemi e detengono un forte potere sulle autorità pubbliche. Quindi, oltre ad avere un peso economico determinante, questi colossi digitali possono condizionare ampiamente le autorità pubbliche, limitandone l'accesso a queste tecnologie, indirizzandone la regolamentazione, intervenendo sulle forme di garanzia dei diritti fondamentali e tutelando libertà essenziali come la libertà di espressione. Infine, un'altra area di preoccupazione dei sistemi di riconoscimento biometrico è il loro alto livello di errore statistico e la loro tendenza a discriminare. Questi algoritmi di riconoscimento biometrico causano spesso numerosi errori nella lettura dei volti, soprattutto nei casi che riguardano donne, bambini, persone di colore e persone con disabilità. Pertanto, la crescente commercializzazione di questi sistemi pone un significativo aumento delle violazioni del principio di

non discriminazione. Violazioni di questo tipo testimoniano la fallibilità di queste tecnologie e dovrebbero farci riflettere sulla reale necessità di una loro applicazione massiccia a fronte di rischi così elevati per i diritti alla privacy, alla libertà di espressione e alla garanzia del principio di non discriminazione.

Ordinamento europeo e ordinamento statunitense a confronto

Nella predisposizione di una disciplina in materia di biometria all'interno del contesto occidentale, l'ordinamento europeo e l'ordinamento statunitense adottano due approcci molto differenti. Nel primo abbiamo l'adozione del GDPR, un regolamento in grado di porre una disciplina sulla privacy molto avanzata ed estesa, mentre nel secondo abbiamo una concezione della tutela della privacy dei cittadini statunitensi molto diversa, connotata dall'assenza di qualsiasi forma di regolazione federale in materia di biometria volta a tutelare i diritti dei singoli individui.

Il contesto europeo emerge come un contesto più regolato, con uno dei modelli legislativi più efficaci per porre una tutela estensiva dei dati personali dei suoi cittadini, mentre in generale, negli Stati Uniti la disciplina sulla privacy si connota come un'area emergente del diritto statunitense che manca di una regolamentazione standardizzata a livello federale, che si riflette anche nell'ambito della regolazione dei sistemi di identificazione biometrica.

Nell'ordinamento europeo, il dato biometrico fino all'introduzione del Regolamento UE n. 679/2016 (GDPR) è sempre stato un oggetto sui generis, evocato nelle riflessioni in dottrina, ma mai espressamente definito. Con l'introduzione del GDPR, invece, il dato biometrico ha finalmente ottenuto la sua autonomia concettuale, attraverso un numero circoscritto di disposizioni dall'art. 4, par. 14 GDPR che ne introduce una definizione univoca, agli artt. 6 e 9 GDPR che ne determinano le condizioni di liceità per il trattamento. Infatti, il GDPR classifica i dati biometrici come una categoria particolare di dati personali ai sensi dell'art. 9, nel quale il primo paragrafo sancisce un divieto generale per il loro trattamento, anche se vi sono diverse eccezioni elencate nel secondo paragrafo dello stesso articolo, che specificano i casi in cui questa disposizione può essere disapplicata. Queste disposizioni includono, ad esempio, i casi in cui l'interessato abbia prestato il suo consenso esplicito al trattamento dei dati personali, o se il trattamento sia necessario per motivi di interesse pubblico basati sul diritto dell'Unione o degli Stati membri. Inoltre, il quarto paragrafo dell'art. 9 stabilisce la possibilità per gli Stati membri di introdurre altre condizioni, o limitazioni, relative al trattamento dei dati biometrici. Altre disposizioni del GDPR relative al trattamento dei dati sensibili riguardano le disposizioni generali relative al rispetto dei principi applicabili al trattamento dei dati; la previsione di sanzioni specifiche; il consenso; la notifica delle violazioni dei dati; il diritto di accesso; il diritto

all'oblio; i principi di portabilità dei dati; privacy by design e l'obbligo per le aziende di designare un responsabile del trattamento. Tuttavia, alcuni elementi tecnici essenziali come la raccolta, l'immagazzinamento e la conservazione di questi dati non sono affrontati in dettaglio e gli Stati membri sono lasciati soli nell'adottare regole nazionali aggiuntive, più severe e specifiche, che ad oggi si dimostrano le più urgenti per affrontare la regolamentazione del mercato relativa a queste tecnologie. In cinque delle dieci esenzioni dell'articolo 9, par. 2 GDPR, è richiesta una legislazione aggiuntiva dell'UE o degli Stati membri per fornire garanzie per i diritti e gli interessi fondamentali dei cittadini europei. L'attività del legislatore europeo dovrebbe essere coadiuvata dalle sinergie dei legislatori dei singoli Stati membri per integrare la disciplina all'interno del proprio diritto nazionale (specialmente per quanto concerne i profili della loro raccolta e conservazione in banche dati). Tuttavia, nel contesto europeo, nessuno Stato membro ha ancora elaborato e introdotto un quadro giuridico di livello primario per i sistemi biometrici. La mancanza di una legislazione nazionale specifica sulla biometria che integri il modello europeo riflette le difficoltà che questi sistemi pongono ai nostri legislatori. Inoltre, il trattamento di queste tecnologie algoritmiche proviene da contesti geografici significativamente diversi, il che complica ulteriormente la determinazione della giurisdizione competente per le controversie in materia. Tutti questi elementi contribuiscono a rallentare l'aggiornamento della disciplina della responsabilità civile derivante dalle inefficienze di queste tecnologie per individuare il soggetto responsabile a cui attribuire gli eventuali danni. Questo complesso quadro giuridico nazionale e sovranazionale si rivela particolarmente oneroso per le aziende che utilizzano questi dati. Di qui, l'obiettivo di trovare un equilibrio tra la libera circolazione dei dati biometrici e la protezione dei cittadini non sembra ancora essere stato raggiunto.

D'altro canto, nell'ordinamento statunitense si assiste ad un approccio diametralmente opposto, che riflette una politica liberista volta a prediligere un approccio "*laissez fare*", piuttosto che un intervento mirato con una rigida disciplina sulla privacy che rischi di ingessare il mercato digitale. La tutela dei diritti del soggetto privato si determina prevalentemente in funzione della facilitazione di queste dinamiche di mercato, non prevedendo una regolazione federale sulla biometria e lasciando un ampio spazio di autonomia ai singoli stati. I principali istituti sulla privacy attualmente in vigore sono le leggi federali del *Federal Trade Commission Act* (FTC), il *Gramm-Leach-Bliley Act* (GLBA) e l'*Health Insurance Portability and Accountability Act* (HIPAA). Nessuno di questi strumenti normativi dispone però una disciplina puntale sulla raccolta e l'utilizzo di dati biometrici; pertanto l'attuale quadro giuridico statunitense sull'identificazione e autenticazione di dati biometrici è caratterizzato esclusivamente dalla predisposizione di singole leggi statali. Attualmente negli Stati Uniti esistono unicamente tre leggi nazionali in materia di biometria promulgate dagli stati dell'Illinois, Texas e Washington, a cui deve essere aggiunta l'esperienza del *California Consumer*

Privacy Act e di alcuni disegni di legge in corso di elaborazione in altri stati. Anche il *Commercial Facial Recognition Act* proposto nel 2019 da due senatori statunitensi, ha segnato un'esperienza significativa. L'esperienza di queste leggi nazionali di fatto pone alcuni principi di base che possono orientare l'implementazione di una regolazione federale in materia, quali i requisiti di informativa e consenso per la raccolta di informazioni biometriche, i requisiti di conservazione e successiva eliminazione del dato, i requisiti per la vendita e la divulgazione di informazioni biometriche e la scelta dei possibili rimedi esperibili dal soggetto per tutelarsi rispetto alle violazioni della propria privacy. Ognuno di questi elementi viene regolato in modo autonomo all'interno della legislazione dei tre stati, tanto che le forti asimmetrie nei diversi modelli adottati rendono sempre più difficile per le aziende adeguarsi alla loro disciplina per non incorrere in sanzioni.

A causa della mancanza di un'uniformità, le aziende possono risultare conformi alla disciplina di uno stato e incorrere in sanzioni in un altro, rendendo per quest'ultime estremamente difficile inserire nuovi prodotti sul mercato senza il rischio di essere sanzionate. Fra questi infatti lo stato dell'Illinois, che con la legge BIPA ha adottato il modello di legislazione più avanzato in materia, è l'unico stato ad attribuire un effettivo potere ai singoli individui attribuendogli la possibilità di esperire ricorsi giudiziali. La sua portata, tuttavia, risulta limitata ai territori del suo stato e nonostante il BIPA rappresenti il modello più significativo per implementare una disciplina federale sui dati biometrici anche la sua applicazione non è risultata sempre lineare, come abbiamo visto nelle sentenze analizzate, esponendo le aziende a un numero estremamente elevato di ricorsi, senza tutelare in ogni caso in modo adeguato i consumatori.

Un modello che ha catalizzato in particolare l'attenzione dei giuristi statunitensi è proprio il modello del GDPR europeo. Dalla sua implementazione nel 2016, infatti, il GDPR ha orientato un forte dibattito nella dottrina statunitense volto a replicarne alcune disposizioni per incrementare le tutele in materia di privacy nell'ordinamento statunitense e adottare un unico modello di regolazione nella disciplina dei dati biometrici. L'attenzione degli americani per il GDPR europeo è data dal fatto che esso non solo concorre nel rafforzare le leggi sulla privacy nei territori europei, ma consolida anche la protezione dei diritti dei cittadini europei rispetto alle imprese, enti e organizzazioni straniere che vantano interessi economici in Europa. La forte asimmetria nei modelli europeo e statunitense pregiudica infatti anche il lavoro di molte attività economiche americane, che si rivelano spesso troppo inadeguate nell'adottare gli standard di sicurezza necessari in materia di privacy per poter fare affari all'interno dell'Unione europea. Questa situazione è stata aggravata ulteriormente anche dall'adozione della Sentenza Schrems II, che ha invalidato la decisione di adeguatezza della legge statunitense del Privacy Shield, adottata nel 2016 dalla Commissione europea dopo la decadenza dell'accordo Safe Harbor, in quanto la Corte di Giustizia dell'Unione europea ha rilevato la non

conformità rispetto alle disposizioni europee dei trattamenti svolti dagli Stati Uniti, ad eccezione che ad essi siano applicate le garanzie ulteriori previste nel GDPR o clausole contrattuali standard (CSS). Per questo da tempo nella dottrina statunitense si dibatte della possibilità di implementare un modello di regolazione federale in ambito biometrico basato sull'impianto del GDPR europeo, che ne imiti i presupposti essenziali senza incorrere nel rischio di ingessare troppo il mercato digitale statunitense. Alcune disposizioni generali alla base dell'impianto normativo del GDPR potrebbero di fatto essere implementate anche all'interno della disciplina sulla privacy statunitense, specialmente per quanto concerne il trattamento di dati biometrici, per ottenere uno standard nazionale con livelli di sicurezza molto elevati e una disciplina decisamente più severa e articolata. Lo scopo alla base di una simile riforma dovrebbe essere l'ideazione di uno standard nazionale per la regolazione dei trattamenti di dati biometrici uniforme in tutti gli stati, anche se un livello di regolazione così esteso potrebbe ottenere anche l'effetto indesiderato di ingessare eccessivamente il mercato digitale statunitense, con oneri burocratici troppo gravosi per le aziende. Sia l'adozione di sanzioni elevate come disposte nel GDPR che l'adozione di un requisito sul consenso così esteso avrebbero un forte potere dissuasivo nei confronti delle aziende, spingendole a conformarsi attentamente alle disposizioni per evitare ogni possibile contenzioso. Inoltre, introdurre la possibilità di poter ritirare facilmente il proprio consenso al trattamento, agevolerebbe gli individui nel disporre di un controllo effettivo sui propri dati.

I diritti individuali introdotti dal GDPR, invece, aumenterebbero il numero azioni esperibili nei ricorsi giudiziali per tutelare l'individuo rispetto alle violazioni subite, mentre il requisito che gli individui siano informati delle violazioni dei dati entro le settantadue ore, agevolerebbe gli individui permettendogli di reagire tempestivamente in caso di violazione dei dati. Anche conoscere lo scopo e la natura del trattamento, nonché il luogo di conservazione dei dati permetterebbe agli interessati di verificare e correggere eventuali informazioni errate, mentre la possibilità di ottenere una copia gratuita dei dati personali raccolti in formato elettronico consentirebbe agli individui di confrontarsi con l'insieme dei dati raccolti sul loro conto. Così i consumatori sarebbero in grado di determinare chi ha accesso a tali informazioni e come intendono utilizzarle. L'implementazione del principio della *privacy by design*, invece, introdurrebbe oneri specifici a carico delle aziende per la corretta messa in sicurezza dei dati all'interno di ogni fase della loro raccolta e successiva conservazione. Le aziende dovrebbero così elaborare solo i dati strettamente necessari per il perseguimento dei loro scopi e limitare contestualmente l'accesso ai dati non necessari. In un contesto in cui la monetizzazione dei dati biometrici non fa che svilupparsi a perdita d'occhio, questo requisito si rivelerà cruciale per impedire alle aziende di raccogliere in massa questi dati per scopi di lucro, vendendo a terzi i dati biometrici dei consumatori. L'applicazione dell'approccio del GDPR negli Stati Uniti consentirebbe pertanto ai consumatori di avere un maggiore controllo sulla raccolta, aggregazione e conservazione

dei loro dati biometrici e di attribuire alle aziende oneri importanti quali la giustificazione della raccolta dei dati e la loro tutela in ogni fase del trattamento attraverso specifici requisiti di sicurezza. Pertanto, ponendo un confronto effettivo fra l'ordinamento europeo e l'ordinamento statunitense, per quanto le disposizioni europee pongano una disciplina del dato biometrico più estesa e efficace, in grado di tutelare in modo più incisivo i diritti e le libertà dei cittadini europei, il modello statunitense detiene comunque alcuni elementi di pregio. Da un lato infatti esso è più attento alle pratiche di mercato, ponendo misure specifiche rivolte esclusivamente alla regolazione dei trattamenti di dati biometrici in ambito commerciale, mentre all'interno del GDPR non vi è un'attenzione specifica per la dimensione commerciale del mercato di questi sistemi biometrici, che invece rappresentano la maggior parte di trattamenti disposti nell'ambito della raccolta di queste tipologie di dati.

Ai sensi dell'art. 9, par. 1 del GDPR, infatti, il trattamento di dati biometrici in ambito commerciale viene fondamentalmente vietato, anche se le condizioni di deroga espresse nel secondo paragrafo di fatto rendono ammissibile questa forma di trattamento. Ai sensi della lettera a) dell'art. 9 par. 2 GDPR il consenso preventivo costituisce l'unica base giuridica in grado di autorizzare il trattamento di dati biometrici all'interno dell'ambito commerciale. Tuttavia, la predisposizione di questa semplice deroga alle disposizioni del par. 1, art. 9, ne depotenzia fortemente la portata e l'estensione della sua disciplina, concedendo di fatto un ampio via libera per queste tipologie di trattamento (ovviamente sempre all'interno delle condizioni di liceità espresse dall'art. 6). Pertanto, nonostante l'ordinamento europeo abbia una definizione puntuale di dato biometrico e una disciplina maggiormente estesa, manca ancora una regolazione specifica per regolare la natura commerciale di questi trattamenti estremamente sensibili e rischiosi per la tutela della privacy dell'individuo.

Dal punto di vista, invece, della regolazione dei trattamenti di dati biometrici da parte di autorità di pubblica sicurezza, se negli Stati Uniti si assiste a una fortissima deregolamentazione di questi sistemi, attribuendo un potere arbitrario estremamente ampio ad agenzie e organi federali e nazionali, in ambito europeo anche l'uso dei sistemi biometrici da parte dei poteri pubblici viene soggetto a regolazione. Nell'Unione Europea l'implementazione del GDPR è stata accompagnata dalla predisposizione della direttiva (UE) 2016/680, nata dall'esigenza di assicurare un livello uniforme ed elevato di protezione dei dati personali delle persone fisiche, agevolando lo scambio di dati personali tra le autorità competenti degli Stati membri, per garantire una maggiore efficacia giudiziaria in materia penale e di polizia. All'interno del testo della suddetta direttiva, il divieto generale di trattamento dei dati biometrici sancito all'art. 9, par. 1 GDPR non viene applicato in tre contesti: nella prevenzione e nella lotta contro la criminalità o nell'esecuzione di sanzioni; nei casi in cui sia necessario prevenire o salvaguardare minacce alla pubblica sicurezza e purché i dati siano trattati dalle Autorità competenti. Inoltre queste Autorità sono autorizzate a predisporre il trattamento di dati

biometrici con finalità di identificazione univoca solo se le tre condizioni cumulative definite all'art. 10 (trattamento di categorie particolari di dati personali) sono rispettate. In presenza di un quadro giuridico chiaro ed un uso proporzionato di questi sistemi, si è sempre ritenuto fondamentale garantire alle autorità di polizia l'accesso a queste tecnologie in funzione della tutela della pubblica sicurezza. L'accesso a immagini facciali, impronte digitali o altri dati biometrici, se configurato all'interno di un'esigenza di interesse pubblico si può ritenere un'ingerenza necessaria nella vita delle persone per consentire di individuare e perseguire crimini, identificare sospetti e agevolare indagini giudiziarie. Attualmente, agenzie europee quali l'Eurodac e L'Europol dispongono quotidianamente la raccolta di dati biometrici di cittadini europei e non solo, all'interno di politiche di sicurezza in materia di immigrazione clandestina o per la creazione di una banca dati biometrica comune a livello europeo fra le varie forze di polizia nazionali. Anche se questi dati non sono necessariamente impiegati in funzioni di controllo una volta acquisiti, la loro raccolta e conservazione può costituire un'interferenza sproporzionata con il diritto alla vita privata delle persone, tanto più se sottoposti a forme di trattamento automatizzate e conservati in database di polizia. Per questo spetta pertanto al diritto nazionale dei singoli Stati membri regolamentare dettagliatamente la registrazione e la conservazione di questi dati per scopi di identificazione biometrica da parte di autorità pubbliche.

Ad oggi una regolamentazione accurata sulla conservazione dei dati biometrici risulta ancora prevalentemente assente nel diritto nazionale degli Stati europei, nonostante l'esponenziale aumento della creazione di queste banche dati ed il rischio crescente di una loro raccolta senza una chiara base legale. Lo stato attuale della disciplina statunitense in materia di biometria, invece, si focalizza esclusivamente sui trattamenti di dati biometrici effettuati per scopi commerciali da imprese private. Di fatto, nell'ordinamento statunitense non esiste una definizione esplicita del concetto di trattamento di dati come nella disciplina europea e non si suddividono le forme di trattamento sulla base del loro ambito di applicazione, ma si dispone esclusivamente una differenziazione sulla base dell'uso pubblico o privato di queste tipologie di dati sensibili, dove se i trattamenti di dati biometrici per scopi commerciali risultano almeno disciplinati in parte attraverso l'esperienza delle leggi nazionali adottate da vari stati, dal punto di vista di un uso pubblico di questi dati da parte di organi e agenzie governative statali e federali si assiste, invece, alla totale assenza di ogni forma di regolazione. Eppure vi è un numero sempre più elevato di soggetti pubblici attivamente coinvolti nel trattamento di dati biometrici per finalità di prevenzione del crimine, sicurezza e contrasto al terrorismo, di cui possono disporre indiscriminatamente senza dover giustificare le loro finalità e senza dover incorrere in alcun tipo di limitazione. Nello specifico, il governo federale porta avanti da tempo iniziative di raccolta di dati biometrici, ad esempio, attraverso il programma NGI e il *Biometric Center of Excellence* fondati dall'FBI, le attività dell'Ufficio di gestione dell'identità biometrica (OBIM) presso il Dipartimento

per la Sicurezza Nazionale del Governo federale, il programma US-VISIT per monitorare gli accessi al paese, la *Secure Communities initiative* dell'ICE e il Sistema Automatico di identificazione biometrica IDENT. L'assenza di un sistema di regole chiare nell'adozione dei sistemi di riconoscimento biometrico si rivela assai controversa. Infatti queste tecnologie predittive possono interferire notevolmente nella tutela della privacy delle persone coinvolte, mettendo in atto vere e proprie azioni di controllo e profilazione. Dove non vi sono limiti chiari nel regolare l'uso di questi sistemi da parte del potere pubblico, vi è il rischio che questo potere possa rivelarsi arbitrario e tradire le sue finalità originarie di sicurezza e interesse pubblico. Per questo, analogamente al caso europeo con la risoluzione adottata il 6 ottobre 2021, anche negli Stati Uniti recentemente si è aperta una discussione sull'eventualità di apporre un vero e proprio divieto sull'uso del riconoscimento facciale all'interno degli spazi pubblici da parte di autorità di pubblica sicurezza, culminato in una serie di provvedimenti nazionali volti a limitare l'impiego di tecnologie di riconoscimento facciale da parte delle autorità locali. Dunque, nonostante l'approccio europeo e statunitense differiscano notevolmente nella predisposizione di un modello di regolazione dei sistemi di riconoscimento biometrico, a fronte di un mercato digitale sempre più globale risultano strettamente interrelati. Per questo, risulta fortemente auspicabile l'introduzione nella disciplina statunitense di alcuni istituti in materia della privacy disposti della disciplina europea, anche alla luce dei rinnovati ostacoli disposti dalla sentenza Schrems II. Inoltre, anche la recente pubblicazione della proposta di Regolamento sull'approccio europeo all'Intelligenza Artificiale porrà sfide ulteriori alla commercializzazione di questi sistemi tra mercato europeo e marcato statunitense. Essa, infatti, nonostante debba essere ancora approvata, pone le basi per un vero e proprio piano di modernizzazione della disciplina europea in campo biometrico, focalizzandosi in particolare sull'uso a fini identificatori di questi sistemi. L'approccio così codificato dal legislatore europeo sembra configurarsi come più votato ad uso etico di queste tecnologie ormai imprescindibili nel nostro quotidiano. Inoltre, all'interno questo mosaico giuridico, di cui tale regolamento costituirà l'ultimo tassello, si cercherà non solo di favorire le opportunità che l'IA offre per le istituzioni, ma anche di valutarne approfonditamente i rischi e le responsabilità che i fornitori di beni e servizi dovranno assumersi all'interno di questo settore, andando probabilmente a incrementare ulteriormente i requisiti necessari per il trattamento di questi dati all'interno di banche dati estere.

I dati biometrici nell'ordinamento italiano

Da ultimo, anche l'analisi della disciplina in materia di dati biometrici all'interno dell'ordinamento italiano si rivela essenziale per mettere a fuoco le strategie adottate dal nostro paese nel recepimento

delle disposizioni europee in materia di biometria e nell'introduzione di una vera e propria disciplina nazionale più estesa rispetto a quella europea. L'esperienza italiana nella regolazione di questi sistemi è stata determinata sia dal recepimento interno delle disposizioni europee attraverso il d.lgs. n. 101/2018, che agli articoli 6 e 7 del Codice Privacy disciplina i dati biometrici, che dal ruolo fondamentale ricoperto dal Garante per la protezione dei dati personali. Infatti, anteriormente all'adozione del GDPR europeo, la disciplina italiana in materia di biometria era regolata dal Provvedimento generale e dalle Linee guida adottate dal Garante nel 2014, che tutt'oggi risultano ancora parzialmente in vigore ai sensi della disciplina transitoria posta dall'art. 22, comma 11 d.lgs. n. 101/2018, che dispone come alcune disposizioni del Codice relative al trattamento di dati biometrici possano continuare a trovare applicazione, in quanto compatibili con il GDPR, fino all'adozione delle corrispondenti misure di garanzia di cui all'articolo 2-septies Codice privacy. Successivamente all'adozione del GDPR e al suo recepimento nel nostro ordimento, il Garante ha continuato a ricoprire un ruolo di primaria importanza nel garantire la sua corretta implementazione, supervisionando l'attività di soggetti pubblici e privati. Tramite numerosi provvedimenti, come nel caso dell'Università Bocconi legato all'utilizzo del software *Respondus* o nelle sanzioni disposte nei confronti di un'Asl provinciale che disponeva l'utilizzo di dati biometrici per rilevare indebitamente le presenze dei suoi dipendenti, il Garante ha contribuito a consolidare la disciplina italiana in materia di biometria favorendone una corretta interpretazione e applicazione. Tuttavia, l'aspetto più saliente rispetto alla regolazione dei sistemi biometrici, è legato al ruolo cruciale che la nostra Autorità dovrà ricoprire in un'ottica futura nel tutelare il benessere delle persone, educarle e trasformarle in soggetti attivi in grado di giocare un ruolo primario nella regolazione di questi sistemi invasivi, attraverso la predisposizione di segnalazioni e reclami. Se le assemblee legislative giocheranno un ruolo cruciale nella definizione degli orientamenti futuri in materia di biometria, le autorità di controllo, in virtù del loro potere indipendente, potranno continuare a valutare in concreto i singoli trattamenti ammettendo solo quelli che in virtù dei principi sanciti dal GDPR risultino giustificabili in termini di liceità, necessità e proporzionalità, in relazione alle finalità perseguite. Anche le modifiche al Codice della privacy introdotte dall'art. 9 del d.l. 8 ottobre 2021, n.139 denominato "DL Capienze", si rivelano interessanti in quanto oltre a incidere sui poteri del Garante, attribuiscono alle pubbliche amministrazioni la possibilità di trattare, comunicare e diffondere dati personali. Questo intervento normativo molto criticato è stato modificato con la legge di conversione n. 205/2021, recante fra le altre misure una parziale moratoria (fino al 31 dicembre 2023) sull'uso di sistemi di riconoscimento biometrico all'interno di spazi pubblici, ispirata alla risoluzione adottata dal Parlamento europeo il 6 ottobre 2021. Sulla base delle nuove disposizioni, inoltre, il trattamento di dati particolari, che prima era concesso per motivi di interesse pubblico rilevante solo nei casi previsti dalla legge, potrà ora

essere regolato anche da un atto amministrativo generale, ai sensi dell'art. 9 del DL Capienze. Nel complesso di questo quadro giuridico nazionale e sovranazionale, con l'adozione delle disposizioni di garanzia sancite all'articolo 7 del Codice Privacy, anche l'Italia avrà la possibilità di adottare un proprio modello di regolazione dei sistemi di riconoscimento biometrici, incidendo sulle strategie di policy-making adottate a livello europeo.

Bibliografia

Anderson M. J., Halpert J., *Washington Becomes the Third State with a Biometric Privacy Law: Five Key Differences,* in *RAIL: The Journal of Robotics, Artificial Intelligence & Law*, 2018, 1(1), 41-46

Andra B., *Facing the Facts on Biometric Phone Locks: Your Face and Thumb Are Not* Secure, in *University of Illinois Journal of Law, Technology &* Policy, 2018, 2, 407-432

Andrew J., Baker M., *The General Data Protection Regulation in the Age of Surveillance Capitalism*, in *Journal of Business Ethics*, 2021, 168, 565-578

Angeles L. P., *Untang Me: Why Federal Judges Are Broadly Construing Illinois's Biometric Privacy Law*, in *Cardozo Law* Review, 2020, 42(1), 349-388

Bacchini F., Lorusso L., *Race, again: how face recognition technology reinforces racial discrimination*, in *Journal of Information, Communication and Ethics in Society*, 2019, Vol. 17(3), 321-335

Beduschi A., *Rethinking digital identity for post-Covid-19 societies: Data Privacy and human rights considerations,* in *Cambridge University Press*, 2021, 3, 1-15

Bellomo G., *Biometria e digitalizzazione della pubblica amministrazione*, in S. Civitarese Matteucci, L. Torchia (a cura di), *La tecnificazione*, Firenze University Press, Vol. 4, 2016

Benson B., *Fingerprints Not Recognized, Why the United States Needs to Protect Biometric Privacy*, in *North Carolina Journal of Law & Technology,* 2018, 19(4), 161-192

Bolognini L., Pelino E., *Codice privacy: tutte le novità del d.lgs. 101/2018: in vigore dal 19 settembre 2018,* Il Civilista, Giuffrè Francis Lefebvre, 2018

Bolognini L., Pelino E., *Codice della Disciplina Privacy,* Giuffrè Francis Lefebvre, 2019

Boyne S. M., *Data Protection in the United States*, in *The American Journal of Comparative Law*, 2018, 299–343

Bud A., *Facing the future: the impact of Apple FaceID*, in *Biometric Technology Today*, 2018, n. 1, 5-7

Buffa F., *Firme elettroniche e grafometriche, dalla direttiva CE/1999/93 al Regolamento eIDAS 2014/910/UE, in vigore dall'1.7.2016*, Editore Key, Cedon Book, 2016

Buresh D. L., *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, in *Santa Clara High Technology Law Journal*, 2021, 38 (1), 39-94

Cinnamon J., *Social Injustice in Surveillance Capitalism*, in *Surveillance & Society*, 2017, 15(5), 609-625

Claypoole T., Stoll C., *Developing Laws Address Flourishing Commercial Use of Biometric Information*, in *Business Law Today*, 2016, n. 5, 1-5

Cohen D., *HIPAA Reform of a Patchwork Scheme: A Look at Preemption, Scope, and the Inclusion of a Private Right of Action in a New Federal Data Privacy Law*, in *American University Whasington College of Law*, 2020, 1-26

Das R., *The science of Biometrics: Security technology for identity Verification*, Routledge, 2019

Dendir S., Maxwell R. S., *Cheating in online courses: Evidence from online proctoring*, in ELSEVIER, *Computers in Human Behavior Reports*, 2020, 1-10

Di Resta F., *La nuova "Privacy europea", i principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, G. Giappichelli Editore, 2018

Ducato R., *I dati biometrici*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, G. Chiapparelli Editore, 2019

Formici G., *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *DPCE online 2/2019*, 2019, 1107-1132

Gardini G., *Le regole dell'informazione, l'era della post-verità,* G. Giappichelli Editore, 2017

Ghelardi E. M., *Closing the Data Gap: Protection Biometric Information under the Biometric Information Privacy Act and the California Consumer Protection Act,* in *St. John's Law Review*, 2020, 94(3), 869-894

Gillis T. B., Spiess J. L., *Big Data and Discrimination*, in *The University of Chicago Law Review*, 2019, Vol. 86, No. 2, 459 -488

Goldman E., *An Introduction to the California Consumer Privacy Act (CCPA)*, in *Santa Clara Univ. Legal Studies Research Paper*, 2020, 1-7

Gonzàlez-Gonzàlez C. S., Infante-Moro A., Infante-Moro J. C., *Implementation of E-proctoring in Online Teaching:A Study about Mitivational Factors*, in *Sustainability*, MDPI, 2020, 1-13

Greco L., Mantalero A., *Industria 4.0, Robotica e Privacy-by-design,* in *Il diritto dell'informazione e dell'Informatica,* 2018, Anno XXXIX Fasc. 6, 875-900

Hartzog W., *BIPA: The Most Important Biometric Privacy Law in the US?*, in *Northeastern University School of Law*, 2021, 409, 96-103

Hert P., Christianen K., *Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric data*, Tilburg University, 2013, 1-57

Hylton K., Levy Y., Dringus L. P., *Utilizing webcam-based proctoring to deter misconduct in online exams*, in ELSEVIER, *Computers & Education 92-93*, 2016, 53-63

Iannuzzi A., Filosa F., *Il trattamento dei dati genetici e biometrici,* in S. Scagliarini (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali, la normativa italiana dopo il d.lgs. n. 101/2018*, Collana Fondazione Marco Biagi, G. Chiapparelli Editore, 2019

Insler C. N., *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, in *Southern Illinois University Law Journal*, 2019, 43(4), 819-826

Insler C. N., *How to Tackle Litigation under the Biometric Information Privacy Act*, in *The Computer & Internet Lawyer*, 2018, 35 (12), 1-5

Jain A. K., Flynn P., Ross A. A., *Handbook of biometrics*, Springer, 2007

Jasserand C., *Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data*, in *European Data Protection Law Review (EDPL)*, 2016, 2(3), 297-311

Kassin S. M., Dror I. E., Kukucka J., *The forensic confirmation bias: Problems, perspectives, and proposed solutions,* in *Journal of Applied Research in Memory and Cognition*, 2013, 2, 42-52

Kindt E.J., *Having yes, using no? Abaout the new legal regime for biometric data,* in *Computer Law & Security Review 34*, 2018, 523-538

Kindt E.J., *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, Springer, 2013

Lenti M. R., *Dati biometrici, firma grafometrica e contratti elettronici. Quali implicazioni per la Cyber Security,* in *LUISS Law Review*, 2017, n. 2, 109-125

Lindqvist J., *New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a World of the Internet of Things?,* in *International Journal of Law and Information Technology*, 2018, 26, 45-63

Llaneza C., *An Analysis on Biometric Privacy Data Regulation: A Pivot towards Legislation Which Supports the Individual Consumer's Privacy Richts in Spite of Corporate Protections*, in *St. Thomas L. Rev.*, 2020, 32(2), 177-198

Logan I. T., *For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection,* in *Penn State Law Review*, 2019, 123(3), 779-812

Lucchini Guastalla E., *Privacy e Data Protection: principi* generali, in V. Franceschelli, E. Tosi (a cura di), *Privacy Digitale, Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Diritto delle nuove tecnologie, Giuffrè Francis Lefebvre, 2019

Lynch J., *Form Finger Prints to DNA, Biometric Data Collection in U. S. Immigrant Communities and Beyond*, in *Immigration Policy Center*, 2012, 1-23

McMahon M., *Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts,* in *Legal Studies Research Paper Series*, 2021, 65, 1- 48

Memon N., *How Biometric Authentication Poses New Challenges to Out Security and Privacy*, in *IEE Signal Processing Magazine*, 2017, Vol. 4, n. 4, 196 -197

Mensi M., La sicurezza cibernetica, in M. Mensi, P. Falletta, *Il diritto del web*, Wolters Kluwer, CEDAM, 2018

Metzger A. L., *The Litigation Rollercoaster of BIPA: A comment on the Protection on Individuals from Violations of Biometric Information Privacy*, in *University of Chicago Law Journal*, 2019, n. 50, 1051-1100

Mobilio G., *I sistemi di identificazione biometrica a distanza: un esempio paradigmatico delle sfide lanciate dalla tecnologia al diritto costituzionale,* in *Consulta Online*, 2021, Fasc. III, 738-748

Monajemi M., *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information,* in *University of Miami International and Comparative Law Review*, 2018, 25(2), 371-408

Mulligan S. P., Freeman W. C., Lineaugh C. D., *Data Protection Law: An Overview*, in *Congressional Research Service*, 2019, 1-79

Navone G., *Il valore giuridico della firma grafometrica*, in *Osservatorio del diritto civile e commerciale*, 2018, Fasc. I, 107-126

Nguyen F. Q., *The Standard for Biometric Data Protection*, in *Journal of Law & Cyber Warfare*, 2018, Vol. 7, n. 1, 61-84

Paolucci F., *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 2021, 204-217

Pardau S. L., *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States,* in *Journal of Technology Law & Policy*, 2020, 23(1), 68-114

Pope C., *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protection Biometric Data*, in *Journal of Law and Policy*, 2018, 26(2), 769-804

Roberg-Perez S., *The Future in Now: Biometric Information and Data Privacy,* in *Antirtust*, 2017, 31(3), 60-65

Robles J., *Patel v. Facebook, Inc.: the Collection, Storage, and Use of Biometric Data as a Concrete Injury under BIPA,* in *Golden Gate University Law Review*, 2020, 50(1), 61-viii

Rodrigues A. K., Fedeles E. R., Martin M. E., *Existing and Emerging Biometric Data Technologies*, in A. Taal, *The GDPR Challenge: Privacy Technology and Compliance in an Age of Accelerating Change*, CRC Press, 2021

Romanou A., *The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise*, in *Computer Law & Security Review 34*, 2018, 99-110

Scheel S., *Autonomy of Migration? Appropriating Mobility within Biometric Border Regimes*, Routledge, 2019

Schwartz R., *Patel V. Facebook, Inc: Biometric Data Collection Changes the Interpretation of Concrete Injury for Intangible Harms*, in *Tulane Journal of Technology and Intellectual Property*, 2020, 22, 263-272

Shatz S., Chylik S. E., *The California Consumer Privacy Act of 2018: A Sea Change in The Protection of California Consumers' Personal Information,* in *Business LAw.*, 75, 2020, 1917-1924

Soffientini M., *Privacy, protezione e trattamento dei dati*, IPSOA Manuali, 2018

Smith P., *BIPA: What Does It Stand for?,* in *Chicago Kent Law Review*, 2020, 95(3), 833-858

Sprokkereef A., *Data Protection and the Use of Biometric Data in The EU*, in S. Fischer-Hubner, P. Duquenoy, A. Zuccato, L. Martucci, *The Future of Identity in The Information Society*, IFIP International Federazion for Information Processing, Volume 262, Boston, Springer, 2008, 277-284

Stepney C., *Actual Harm Means It Is Too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law*, in *Layola of Los Angeles Entertainment Law Review*, 2019, 40(1), 51-88

Stewart L., *Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security,* in *Boston College Law Review*, 2019, 60(1), 349-386

Strycharz J., Ausloos J., Helberger N., *Data Protection or Data Frustration? Individual Perceptions and Attitudes towards the GDPR*, in *European Data Protection Law Review (EDPL)*, 2020, 6(3), 407-421

Swafford J., *Rosenbach v. Six Flags Entertainment Corp.*, in *Federal Communications Law Journal*, 2020, 72(2), 297-299

Tosi E., *Diritto privato delle nuove tecnologie digitali, Riservatezza, contratti, responsabilità tra persona e mercato*, Diritto delle nuove tecnologie, Giuffrè Francis Lefevbre, 2021

Trebble-Greening J., *Rasing the Stakes: Creating an International Saction to Generate Corporate Compliance with Data Privacy Laws*, in *Columbia Business Law Review*, 2019, 2, 763-796

Tropea G., *Recensione a S. Zuboff, Il Capitalismo della sorveglianza. Il futuro dell'umanità dell'era dei nuovi poteri, Roma, Luiss University Press, 2019 (con una postilla su Privacy e Covid-19)*, in *P.A. Persona e Amministrazione*, 2020, 479-491

Van Natta M., Chen P., Herbek S., et al., *The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic*, in *J. Law Biosci*, 2020, 1-17

Woldeab D., Brothen T., *Online Proctoring, Test Anxiety and Student Performance*, in *Internazional Journal of E-learning & Distance Education*, 2019, Vol. 34, No. 1, 1-10

Wong K.A., *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation,* in *20 J. High Tech*, 2020, l. 229, 229-269

Zaccaria R., Valastro A., Alabanesi E., *Diritto dell'informazione e della comunicazione*, Milano, Wolters Kluwer, CEDAM, 2018

Zimmerman H., *The Data of You: Regulating Private Industry's Collection of Biometric Information*, in *University of Kansas Law Review*, 2018, 66, 637-672

Zuboff S., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, 2019

Zuboff S., *Surveillance Capitalism anf the Challenge of Collective Action,* in *New Labor Forum*, 2019, 28(1), 10-29

Zuboff S., Möller N., Murakami Wood D., Lyon D., *Surveillance Capitalism: An Interview with Shoshana Zuboff*, in *Surveillance & Society*, 2019, 17 (1/2), 257-266

Sitografia

Agenzia per l'Italia Digitale (AGID)
https://www.agid.gov.it/it

Ahlering T., Maatman G., *Maryland Joins Growing Number of States Introducing Biometric Information Privacy Bills With Potential to Spur Class Action Litigation*, in *JDSUPRA*, 24 febbraio 2021
https://www.jdsupra.com/legalnews/maryland-joins-growing-number-of-states-3182422/

Barber G., *San Francisco Bans Angency Use of Facial-Recognition Tech*,in *Wired*, 14 may 2019
https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/

Bassini M., *DL Capienze, perché indebolire la privacy? I dubbi di forma e di sostanza*, in *Agenda* Digitale, 9 novembre 2021
https://www.agendadigitale.eu/sicurezza/privacy/dl-capienze-perche-indebolire-la-privacy-i-dubbi-di-forma-e-di-sostanza/

Bocconetti S., *L'europarlamento contro la sorveglianza di massa nei luoghi pubblici*, Il Manifesto, 6 ottobre 2021
https://ilmanifesto.it/leuroparlamento-contro-la-sorveglianza-di-massa-nei-luoghi-pubblici/

Carrer L., *La moratoria sul riconoscimento facciale approvata in Italia ci ricorda perché dobbiamo chiedere un divieto*, articolo pubblicato sul sito del centro di ricerca Hermes, 2 dicembre 2021
https://www.hermescenter.org/italia-moratoria-riconoscimento-facciale-ban-divieto/

Centro di ricerca Hermes
http://www.hermesricerche.it

Commissione europea
https://ec.europa.eu/info/index_it

Consiglio d'Europa
https://www.coe.int/it/web/portal/home

Corte di Giustizia dell'Unione europea
https://curia.europa.eu/jcms/jcms/j_6/it/

DeGeurin M., *Amazon's Facial Recognition Software Mistakes 28 Cogressmen for Criminals*, , Intelligencer, New York Magazine, 27 luglio 2018
https://nymag.com/intelligencer/2018/07/amazon-rekognition-mistakes-congressmen-for-criminals-aclu.html

Duportail J., *I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets*, in *The Guardian*, 26 settembre 2017
https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold

Eurodac, pagina ufficiale del Dipartimento per le Politiche europee
https://www.politicheeuropee.gov.it/it/comunicazione/euroacronimi/eurodac/

European Data Protection Board
https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_it

Federal Bureau of Investigation (FBI)
https://www.house.gov/

Garante per la protezione dei dati personali
https://www.garanteprivacy.it/home

Hern A., *IBM quits facial-recognition market over police racial-profiling concerns*, in *The Guardian*, 9 giugno 2020
https://www.theguardian.com/technology/2020/jun/09/ibm-quits-facial-recognition-market-over-law-enforcement-concerns

Hill K., Mac R., *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, in *New York Times*, 5 november 2021
https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html

Levine E. S. et al., *The New York City Police Department's Domani Awareness System*, in *Informs Journal on Applied Analytics*, 18 gennaio 2017
https://pubsonline.informs.org/doi/10.1287/inte.2016.0860

Lust K. L., Galibois M., Lefebvre J., *New York proposes a new Biometric Privacy Act*, in *Technology Law Dispatch*, 11 gennaio 2021
https://www.technologylawdispatch.com/2021/01/privacy-data-protection/new-york-proposes-a-new-biometric-privacy-act/

Martorana M., *Trattamento dei dati biometrici e utilizzi in ambito commerciale*, in *Altalex*, 18 febbraio 2021
https://www.altalex.com/documents/news/2021/02/18/trattamento-dei-dati-biometrici-e-utilizzi-in-ambito-commerciale

New York Police Department (NYPD)
https://www1.nyc.gov/site/nypd/index.page

Parlamento europeo
https://www.europarl.europa.eu/portal/it

Pelino E., *Riconoscimento facciale, perché la moratoria non basta: tutti i nodi della norma italiana*, in *Agenda Digitale*, 6 dicembre 2021
https://www.agendadigitale.eu/sicurezza/privacy/riconoscimento-facciale-perche-la-moratoria-non-basta-tutti-i-nodi-della-norma-italiana/

Pizzetti F., *Il Nuovo Comitato europeo per la protezione dei dati (EDPB), dopo il GDPR: compiti e poteri*, in *Agenda Digitale*, 31 maggio 2018
https://www.agendadigitale.eu/sicurezza/il-nuovo-comitato-europeo-per-la-protezione-dei-dati-edpr-dopo-il-gdpr-compiti-e-poteri/

Roberts J. J., *Homeland Security Plans to Expand Fingerprint and Eye Scanning at Borders*, in *Fortune*, 12 settembre 2016
https://fortune.com/2016/09/12/border-security-biometrics/

Simonite T., *Face Recognition Is Being Banned – but It's Still Everyehere*, in *Wired*, 22 dicember 2021
https://www.wired.com/story/face-recognition-banned-but-everywhere/

Singleton K., *Illinois Appellate Court Holds That BIPA Plaintiffs Must Show Actual Harm*, in *JDSUPRA*, 28 marzo 2018
https://www.jdsupra.com/legalnews/illinois-appellate-court-holds-that-62705/

Sito ufficiale della campagna "Ban Facial Recognition in Stores"
https://www.banfacialrecognition.com/stores/

Sito ufficiale della campagna europea "Reclaim Your Face"
https://reclaimyourface.eu

Taneja D., *Whasington Enacts a Biometric Privacy Statute in a Departure from the Existing Standard*, in *New Media and Technology Law Blog*, 13 giugno 2017
https://perma.cc/6F2X-27CA

Towey H., *The retail stores you probably shop at that use facial-recognition technology*, in *Business Insider*, 19 luglio 2021
https://www.businessinsider.com/retail-stores-that-use-facial-recognition-technology-macys-2021-7?r=US&IR=T

U.S. Department of Homeland Security
https://www.dhs.gov/

U.S. House of Representatives
https://www.house.gov/

Whittakaer Z., *FBI can keep secret who's in its biometrics 'mega database' says Justice Dept.,* in *ZDNet*, 8 agosto 2017
https://www.zdnet.com/article/fbi-to-keep-secret-biometrics-database-justice-department/