RICONOSCIMENTO FACCIALE E DATI BIOMETRICI. UNA PRIMA RIFLESSIONE

Giovanni Sciancalepore[1*]

SOMMARIO: 1.- Funzionalità ed applicazioni dei sistemi di riconoscimento facciale; 2.- Dall'immagine al dato biometrico: le informazioni sensibili al vaglio delle nuove tecnologie; 3.- Il problema del consenso "invisibile"; 4.- Quali sfide per la tutela dei diritti fondamentali?

1.- **Funzionalità ed applicazioni dei sistemi di riconoscimento facciale.**

Le tecnologie di riconoscimento facciale (di seguito, TRF) rappresentano strumenti avanzati di verifica biometrica che, attraverso l'impiego di sofisticati algoritmi, consentono di individuare un soggetto muovendo dall'analisi delle caratteristiche uniche del suo viso. Tali sistemi, mediante l'acquisizione di riprese fotografiche o video, sono in grado di rivelare l'identità di una persona grazie ad un processo automatizzato capace di confrontare l'immagine estrapolata con informazioni precedentemente registrate[2].

Le TRF si impongono quale strumento prediletto per la sorveglianza di massa[3], declinandosi in una molteplicità di applicazioni che spaziano dalla sicurezza pubblica

[1*] Professore ordinario di Sistemi giuridici comparati presso il Dipartimento di Scienze Giuridiche (Scuola di Giurisprudenza) dell'Università degli Studi di Salerno.

[2] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli 2021, 11; M. Mann, M. Smith, *Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight*, in *University of New South Wales Law Journal* 1 (2017) 121ss.; A. Orlando, *La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea IActa est?*, in *DPCE online* 2 (2024) 1111.

[3] Con il termine "sorveglianza di massa" si può intendere la «raccolta ed elaborazione di dati personali, identificabili o meno, allo scopo di influenzare o controllare coloro ai quali essi appartengono». Da un lato, il fenomeno si configura nella sua dimensione positiva come esercizio di cura e protezione volto a salvaguardare il benessere e la sicurezza di individui o collettività. In questa prospettiva, essa trova legittimazione in contesti quali l'assunzione di responsabilità genitoriale, dove la tutela dei minori richiede un monitoraggio continuo; negli ambienti lavorativi, per garantire il rispetto di normative di sicurezza e produttività; nell'operato degli organi governativi, che si impegnano a garantire la sicurezza pubblica e la stabilità sociale. Tuttavia, tale pratica, quando si declina nella sua versione più coercitiva, diviene uno strumento per limitare le libertà individuali e comprimere i diritti fondamentali. Nella capacità di imporre restrizioni e controlli si nasconde il rischio di trasformare la sorveglianza in un meccanismo di oppressione, in cui la protezione si trasfigura in dominio e il monitoraggio si converte in un'occasione per consolidare poteri arbitrari e sottrarre agli individui il controllo sui propri dati e sulla propria autonomia. Questa ambivalenza esige una riflessione profonda sull'equilibrio tra tutela e invasività, affinché la sorveglianza

all'analisi comportamentale, fino al monitoraggio su scala globale e all'ottimizzazione di servizi personalizzati. La loro diffusione risulta giustificata dalla facilità con cui è possibile conseguire simili dati rispetto ad altre forme di riconoscimento, come le impronte digitali, i campioni di DNA o le scansioni dell'iride, che richiedono procedimenti assai più complessi ed invasivi[4].

Per comprendere l'essenza e le implicazioni profonde di siffatte tecnologie, allora, è necessario indagarne le principali finalità operative. Tra queste, vi è certamente l'autenticazione, procedura che opera attraverso un confronto "uno-a-uno". In tale ambito, il "software" analizza l'immagine acquisita e controlla se la stessa corrisponda a quella già nota ed associata ad un'identità determinata. Questo processo è largamente impiegato tanto in contesti specifici, quali lo "screening" aeroportuale, quanto in attività quotidiane in cui, ad esempio, il volto dell'utente sostituisce tradizionali credenziali come "password" o "pin" per accedere ai dispositivi elettronici. Segue poi l'identificazione, dove il raffronto si estende in modalità "uno-a-molti". Nello specifico, il dato viene verificato tra una pluralità di modelli biometrici custoditi in "database". Tale obiettivo, di

non si tramuti in uno strumento pericoloso di lesione delle libertà personali e democratiche. Cfr. D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano 2002; P. Perri, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Milano 2020, 3ss; Mobilio, *Tecnologie* cit. 12ss.

[4] Il procedimento di riconoscimento facciale, pur variando nei dettagli tecnici e nella complessità algoritmica, si snoda attraverso una sequenza articolata di fasi, ciascuna delle quali rappresenta un passo verso la decifrazione dell'identità individuale nel linguaggio informatico. Si inizia con l'acquisizione dell'immagine, momento in cui il volto umano viene immortalato e tradotto in formato digitale. Questo passaggio può avvenire in modo volontario e controllato (cd. sistema biometrico interattivo), come nel caso di foto biometriche ufficiali, oppure in maniera furtiva e involontaria (cd. sistema biometrico passivo) attraverso, ad esempio, videocamere di sorveglianza. Segue, poi, l'individuazione del volto all'interno della scena. In questa fase, il sistema isola il viso dal contesto, distinguendolo dagli elementi dello sfondo. Il processo prosegue con la normalizzazione, in cui si mitigano le distorsioni dovute a variazioni di posizione, illuminazione o angolazione. Attraverso sofisticate tecniche di standardizzazione, il volto viene riportato ad un formato uniforme, facilitando l'identificazione dei cosiddetti punti di riferimento, come occhi, naso e bocca, che diverranno fondamentali nelle analisi successive. L'estrazione delle caratteristiche, poi, rappresenta il cuore del procedimento. Qui si isolano i tratti biometrici distintivi e riproducibili, trasformandoli in un modello digitale unico, chiamato "template biometrico". Il modello così ottenuto viene quindi registrato, arricchendo i "database" con un nuovo elemento di confronto. È grazie a questa "memoria digitale" che il sistema è in grado, nella fase finale del confronto, di mettere in relazione il modello appena creato con quelli già archiviati, svelando somiglianze ed identità con precisione sempre maggiore. Cfr. Garante per La Protezione dei Dati Personali, Linee-guida in materia di riconoscimenti biometrico e firma grafometrica. Allegato A al Provvedimento del Garante 12 novembre 2014, pubblicato in Gazzetta Ufficiale il 2/02/2014, n. 280.

grande rilievo nell'ambito delle operazioni di sicurezza pubblica, consente di rintracciare individui ricercati o identificare soggetti di interesse in ambienti più o meno sorvegliati. Infine, la categorizzazione, che ambisce ad estrarre attributi significativi dall'immagine facciale. In base a caratteristiche come l'età, il sesso o lo stato emotivo, il sistema procede a classificare la persona in gruppi "target". Questo tipo di analisi, spesso impiegata in contesti ludici o commerciali, come le "console" di gioco o il "marketing" digitale, si limita a segmentare il pubblico per ottimizzare esperienze personalizzate.

Occorre, tuttavia, precisare che le TRF si basano su algoritmi probabilistici, capaci di restituire risultati ordinati per grado di somiglianza, ma non esenti da margini di errore. Ogni operazione di riconoscimento, pertanto, non garantisce mai una precisione assoluta, ma è sempre accompagnata da un coefficiente di incertezza che può sollevare dubbi sull'affidabilità e sull'equità delle decisioni derivate. Tali procedure si espongono, infatti, a gravi rischi discriminatori generati dall'inefficienza dei "software", intrisi dei cosiddetti "bias", causando distorsioni significative per l'incapacità di stabilire una corrispondenza affidabile con le immagini archiviate nei "database"[5].

In tale scenario, l'interessato è assoggettato ad un processo identificativo attraverso modalità che spaziano dalla coercizione manifesta sino a forme di analisi più subdole e silenziose: quale inconsapevole protagonista dell'odierno scenario tecnologico, egli si presta alla scansione biometrica per spontanea accondiscendenza, ignorando le implicazioni profonde del proprio assenso, oppure si trova al centro di un processo totalmente invisibile, in cui il suo volto diviene oggetto di tracciamento senza che abbia la benché minima cognizione di quanto stia avvenendo.

[5] L'impiego delle TRF solleva interrogativi di profonda rilevanza sotto il profilo del principio di uguaglianza *ex* art. 3 Cost., pilastro imprescindibile di ogni ordinamento democratico. In ambito lavorativo, ad esempio, alcune imprese già adottano queste tecnologie per valutare i candidati durante i colloqui di assunzione, analizzandone espressioni facciali, tono di voce e comportamento verbale. Questo utilizzo, apparentemente neutro, potrebbe in realtà esacerbare disparità preesistenti, penalizzando soggetti che non si conformano agli "standards" impliciti stabiliti dall'algoritmo. Una tale pratica non solo amplifica le disuguaglianze sociali, ma pone questioni di legittimità rispetto alla libertà di valutazione del datore di lavoro, la quale deve comunque conformarsi ai principi di trasparenza e non discriminazione. Cfr. Mobilio, *Tecnologie* cit. 88ss.

Le criticità legate alle TRF, poi, si amplificano in maniera esponenziale se inserite nel contesto degli strumenti informatici avanzati che ne hanno favorito lo sviluppo, quali l'intelligenza artificiale, i "big data" e il "machine learning".

Questo ventaglio di possibilità solleva interrogativi di straordinaria gravità, sia dal punto di vista tecnico sia giuridico ed etico, poiché la rilevazione morfologica, da atto cosciente e volontario, rischia di trasformarsi in un'operazione di controllo silente e pervasivo, priva di trasparenza e immune al consenso informato. In altre parole, la persona non è più soggetto di diritti, ma diviene mero dato in un sistema che osserva, registra e giudica, in modo del tutto inaccessibile alla sua comprensione e al suo potere di opposizione[6].

Tali nuove forme di vigilanza, tuttavia, non si limitano ad essere esercitate da autorità pubbliche[7], ma, *a contrariis*, si estendono e trovano espressione soprattutto nell'attività incessante di imprese ed operatori privati.

Nel panorama attuale, dominato dalla società dell'informazione, ciascun essere umano si trova sottoposto ad una molteplicità di sorveglianti, ciascuno con finalità differenti, ma accomunati dal medesimo intento: sfruttare i dati personali come risorsa di inestimabile valore, principalmente per scopi di natura commerciale.

A detenere il dominio di questo nuovo ordine di controllo sono le cosiddette "Big Tech"[8], colossi del "web" che incarnano oggi il vero potere di osservazione e di analisi. Si

---

[6] Si veda D. Limone, *Introduzione all'intelligenza artificiale. Materiali per una strategia e una regolamentazione*, in *Rivista elettronica di Diritto, Economia e Management* 4 (2023) 23ss.; F. Pizzetti, *"Dati inferiti", regolarne l'uso per tutelare le persone: la nuova frontiera della privacy*, in *https://www.agendadigitale.eu*.

[7] Nell'ambito delle pubbliche istituzioni, le TRF sono impiegate *in primis* dalle forze dell'ordine con finalità di identificazione e di perseguimento di coloro che si rendono sospetti di aver commesso atti criminosi, nonché per rintracciare persone scomparse. Tali sistemi si rivelano altresì strumentali nell'attività di controllo e vigilanza alle frontiere, in particolare negli aeroporti, dove la necessità di un'identificazione rapida e sicura si fa sempre più pressante, oppure in contesti più complessi, come la gestione delle politiche migratorie ed il coordinamento delle operazioni di rimpatrio, processi che vedono nell'automazione e nella tracciabilità dei movimenti un elemento chiave per le autorità statali e internazionali.

[8] Per quanto concerne i cosiddetti colossi della rete si tende, di solito, ad individuarli nel gruppo americano "GAFA", ovvero Google (e la collegata Alphabet), Amazon, Facebook ed Apple (cui si aggiungono solitamente Microsoft e IBM), e in quello cinese "BAT" (Baidu, Alibaba e Tencent). Essi svolgono un ruolo di primo piano nell'uso degli strumenti di riconoscimento facciale. Si pensi, ad esempio, al noto sistema "Rekognition" di Amazon oppure a quello "Deepface" di Facebook e, non da ultimo, a quello "FaceNet" di Google. In merito ai rischi derivanti dalla posizione assunta dalle "Big Tech", si v. T.E. Frosini, *Internet e democrazia*, in *Dir. inf.* 4-5 (2017) 670; cfr. N. Petit, *Technology Giants, the 'Moligopoly*

configurano, così, come i protagonisti di un inedito paradigma economico, ossia il «capitalismo della sorveglianza»[9], dove la conoscenza dettagliata e la previsione dei comportamenti umani rappresentano la nuova moneta di scambio e il principale strumento di egemonia.

In tale sistema, le aziende tecnologiche raccolgono, processano e monetizzano informazioni personali, trasformando ogni interazione digitale in un'occasione per accumulare dati. Queste attività, spesso occultate dietro l'apparente gratuità dei servizi offerti, celano un prezzo ben più alto: la compromissione della "privacy" e della libertà individuale.

2.- **Dall'immagine al dato biometrico: le informazioni sensibili al vaglio delle nuove tecnologie.**

Nel contesto dei nuovi sistemi cibernetici[10] l'elaborazione dei dati biometrici si impone quale componente invisibile – ma talvolta inevitabile – dell'odierna società dell'informazione.

Hypothesis' and Holistic Competition: A Primer, in *SSRN* 3 (2016) 25ss.; H.S. Mousavi, *Facial recognition: top 7 trends (tech, vendors, markets, use cases & latest news)*, in *Thales* 2 (2020) 46ss.

[9] E. Longo, A. Pin, *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale*, in *Diritto pubblico comparato ed europeo* 1 (2023) 105. Gli Autori evidenziano che «per la conquista del potere non è più necessario possedere i mezzi di produzione, bensì l'accesso alle informazioni che vengono utilizzate per la sorveglianza, il controllo e la previsione dei comportamenti». Cfr. B.C. Han, *La società della trasparenza*, Roma 2014, 83: «La sorveglianza oggi non si realizza, come si ritiene normalmente, nella forma di un attacco alla libertà. Piuttosto, ciascuno si consegna volontariamente allo sguardo panottico. Si collabora intenzionalmente al panottico digitale, svelando ed esponendo se stessi. Il detenuto del panottico digitale è, al tempo stesso, carnefice e vittima. In ciò consiste la dialettica della libertà. La libertà si rivela controllo».

[10] Con riferimento allo sviluppo delle biometrie: S. Amato, *Ai confini del corpo*, in S. Amato, F. Cristofari, S. Raciti, *Biometria: i codici a barre del corpo*, Torino 2013, 5ss.; A.K. Jain, A.A. Ross, *Introduction to Biometrics*, in A.K. Jain, P. Flynn, A.A. Ross (curr.), *Handbook of Biometrics*, New York 2008. Già nel 2010, in ambito nazionale, il Comitato nazionale per la bioetica aveva individuato la "biometria" come una nuova tecnica «di identificazione o "misurazione" dell'essere umano attraverso la rilevazione di determinate caratteristiche fisiche e comportamentali che vengono tradotte in sequenze matematiche e conservate in banche dati elettroniche (…) Lo sviluppo tecnologico ha reso i mezzi e gli strumenti di identificazione estremamente sofisticati, complessi ed efficienti, accrescendo le opportunità e i benefici, ma nello stesso tempo moltiplicando le occasioni di controllo sociale. Il corpo ha assunto il ruolo di una vera e propria "password", ovvero di un codice di riconoscimento vivente che si integra e interagisce col mondo delle macchine». Comitato Nazionale per la Bioetica, L'identificazione del corpo umano: profili bioetici della biometria, 26/11/2010, 3ss.

Ed invero, l'individuazione di un determinato soggetto, attraverso immagini registrate e complessi procedimenti algoritmici automatizzati, si sostanzia in un trattamento di specifiche tipologie di informazioni, riferite a peculiarità morfologiche – *rectius* del volto – uniche e rappresentanti ciascun essere umano[11]. La loro esatta qualificazione, soprattutto se alla luce del costante progresso scientifico e dell'evoluzione tecnologica[12], si rivela dunque requisito essenziale per assicurare una regolamentazione adeguata del fenomeno e salvaguardare in maniera piena ed efficace il diritto di riservatezza coinvolto dalla procedura[13].

Difatti, il rapporto tra le innovazioni digitali – fondate sull'utilizzo di peculiari categorie di dati – e la protezione della "privacy" deve necessariamente costituire un *prius* logico-giuridico[14] rispetto all'esatta applicazione di tali algoritmi ed ai conseguenti rischi per le libertà fondamentali degli interessati[15].

L'intersezione tra ricognizione normativa e pratica informatica, allora, in simili settori non può prescindere da una cornice legislativa puntuale ed articolata, orientata a garantire un giusto equilibrio tra progresso scientifico e tutela individuale.

---

[11] In argomento: Orlando, *La regolamentazione* cit. 1111ss.; Mobilio, *Tecnologie* cit. 136ss.; F. Di Matteo, *La riservatezza dei dati biometrici nello Spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, in *Freedom, security & justice : european legal studies* 1 (2023) 74ss.; S. Del Gatto, *La governance delle nuove tecnologie tra tentativi di regolazione e istanze di "self regulation". Il caso del riconoscimento facciale*, in *Riv. Ital. di diritto pubblico comunitario* (2023) 37ss.; G. Mobilio, *Facial recognition technologies and the next frontiers of interoperability*, in *Medialaws* (2023).

[12] È stato evidenziato in tal senso che, in ragione delle continue acquisizioni della società dell'informazione e dei costanti mutamenti della stessa, appare allo stato difficile rendere una definizione statica e definitiva di dato biometrico. A. Iannuzzi, F. Filosa, *Il trattamento dei dati genetici e biometrici*, in *Dirittifondamentali.it* 2 (2019) 2ss.; Mobilio, *Tecnologie* cit. 138ss.

[13] La necessità di distinguere il trattamento dei dati biometrici dalla categoria più ampia dei dati personali è da sempre stata avvertita dagli operatori del settore. Già, infatti, nel 2003 con l'attività del Gruppo di lavoro per la tutela dei dati personali, istituito a norma dell'art. 29 della Direttiva 95/46/CE, si era ritenuta opportuna l'elaborazione di un documento sui rischi derivanti dal ricorso, generalizzato e incontrollato, della biometria per il riconoscimento e l'identità delle persone, che tenesse correttamente conto della natura delle informazioni trattate e dell'esatta applicazione dell'allora vigente Direttiva 95/46/CE. Sul punto cfr. Gruppo di lavoro per la tutela dei dati personali, Documento di lavoro sulla biometria, 01.08.2003.

[14] In questo senso Di Matteo, *La riservatezza* cit. 80ss.

[15] I rischi a cui si fa riferimento non riguardano esclusivamente eventuali criticità rilevabili in termini di sicurezza dei dati, ma anche ai possibili errori derivanti dai processi di utilizzazione delle informazioni biometriche registrate ed alla potenziale lesione dei diritti fondamentali degli individui.

Sicchè, attesa la peculiare natura "sensibile" delle informazioni sottese a tali meccanismi, ad esse occorre estendere in primo luogo tutto l'*acquis* normativo, internazionale ed europeo, relativo alla salvaguardia dei dati personali che, soprattutto nel quadro giuridico delineato dal diritto dell'Unione europea, sembra apparire, almeno con riferimento all'ambito definitorio, funzionale allo scopo[16].

Nello specifico, l'articolo 4, n. 14 del G.D.P.R. provvede a configurare il possibile trattamento di identificatori biometrici nelle ipotesi di dettagli ottenuti da una gestione tecnica specifica e relativi «alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca»[17]. Dunque, affinché possa operarsi una corretta distinzione rispetto alle informazioni comuni[18], non può prescindersi dalla concomitanza di tre presupposti fondamentali, riferiti alla natura del dato elaborato, ai mezzi ed alle modalità del trattamento usato nonché agli obiettivi dello stesso[19].

Solo, quindi, laddove l'utilizzo della ripresa fotografica[20] – che valga a rappresentare caratteristiche uniche dell'interessato – sia indirizzato, attraverso l'impiego di dispositivi

[16] Cfr. Di Matteo, *La riservatezza* cit. 109. Evidenzia, in particolare, Orlando, *La regolamentazione* cit. 1114: «A questo riguardo, il regolatore si confronta con un quadro normativo che, per quanto bisognoso di costante aggiornamento, è comunque già esistente e consolidato, almeno nelle esperienze oggetto di questo lavoro. Pertanto, anche in questo caso occorrerà verificare se possano essere trovate soluzioni accettabili già *de iure condito* o, se invece, si renda necessario un aggiornamento della disciplina».

[17] Reg. (UE) 27/04/2016, n. 679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE, (G.D.P.R.), art. 4, n. 14: «Ai fini del presente regolamento s'intende per: (…) «dati biometrici»: 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».

[18] Simile attività appare necessaria soprattutto se in considerazione della formulazione ampia e omnicomprensiva del dato personale, C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federlasmi.it* 22 (2018); F. Di Resta, *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e i profili risarcitori*, Torino 2018; S. Sica, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. Sica, V. D'Antonio, G. M. Riccio (curr.), *La nuova disciplina europea della privacy*, Padova 2016.

[19] Comitato Europeo Per La Protezione Dei Dati, Linee guida 03/2019 sul trattamento dei dati personali attraverso dispositivi video, 20/01/2020.

[20] In tal senso, il considerando n. 51 del Reg. (UE) 2016/679 evidenzia che: «Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi

all'uopo progettati, all'individuazione di uno specifico soggetto[21], può discorrersi propriamente di dato biometrico, ricompreso nella categoria di cui all'articolo 9 del G.D.P.R., esposta a peculiari limitazioni e condizioni di legittimità[22].

In altri termini, il requisito perché l'uso delle immagini possa essere qualificato come trattamento sensibile risiede nella funzionalizzazione dell'attività di confronto di caratteri univoci, «mediante l'ausilio di appositi strumenti "software" o "hardware"»[23], tesa per l'appunto al riconoscimento di un determinato soggetto.

In tal senso, quindi, non può essere trascurata, ai fini della giusta riferibilità della disciplina in esame, la preliminare valutazione circa le finalità perseguite da siffatti

significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, essendo inteso che l'utilizzo dei termini «origine razziale» nel presente regolamento non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte. 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 siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro se l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali».

[21] Comitato Europeo Per La Protezione Dei Dati, Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto, 26/04/2023.

[22] Invero, il trattamento dei dati disciplinati dall'art. 9 del G.D.P.R. (tra i quali rientrano anche i dati biometrici) è sostanzialmente vietato, a meno che non sussista una precipua base legale come puntualmente indicata dalla norma.

[23] Garante per la protezione dei dati personali, Verifica preliminare. Riconoscimento via webcam dei partecipanti a corsi di formazione in diretta streaming del 26/07/2017. Ad una conclusione parzialmente differente è pervenuta la Cass., Sez. I, 13/05/2024, ord. n. 12967, sostenendo che «ricorre un trattamento di dati biometrici quando gli stessi sono ottenuti mediante un trattamento tecnico automatizzato specifico, realizzato con un "software" che, sulla base di riprese e analisi delle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, le elabora, evidenziando comportamenti o elementi anomali, e che perviene a un esito conclusivo, costituito da un elaborato video/foto che consente (o che conferma) l'identificazione univoca della persona fisica, restando irrilevante la circostanza che l'esito finale del trattamento sia successivamente sottoposto alla verifica finale di una persona fisica».

sistemi, da individuarsi nella distinzione tra meccanismi di verifica "one-to-one" e strumenti di identificazione "one-to-many"[24].

Benché, infatti, ambedue le funzioni possano sottintendere il trattamento di dati biometrici, occorre in concreto ponderare il risultato raggiunto[25].

Bisogna, quindi, verificare se la tecnologia impiegata ponga in essere una "face recognition" propriamente detta – individuando l'identità del soggetto interessato attraverso il confronto delle caratteristiche fisiche – ovvero si limiti ad una mera "face detention", ossia alla raccolta di riprese raffiguranti volti di persone. Nel caso in cui, infatti, non avvenga una conservazione del "template" biometrico[26], seppur in astratto quanto ottenuto sia adoperabile per il riconoscimento univoco dell'utente, ad esso, laddove manchi il presupposto essenziale della "autenticazione", non potranno riferirsi le regole prescritte in materia di dati biometrici, ma piuttosto le "sole" norme generali a tutela dei dati personali[27].

[24] Cfr. Comitato Europeo, Linee guida cit. 10ss., laddove si precisa che «il riconoscimento facciale può svolgere due funzioni distinte: l'autenticazione di una persona, al fine di verificare che quest'ultima sia chi afferma di essere. In questo caso il sistema confronterà un modello o un campione biometrico preregistrato (memorizzato per esempio su una carta intelligente o su un passaporto biometrico) con un singolo volto, ad esempio quello di una persona che si presenta a un punto di controllo, per verificare se si tratti della stessa persona. Questa funzionalità si basa pertanto sul confronto di due modelli ed è anche detta verifica 1:1; l'identificazione di una persona, al fine di trovarla in mezzo a un gruppo di persone, all'interno di una zona specifica, di un'immagine o di una banca dati. In questo caso, il sistema deve elaborare ogni volto acquisito per generare un modello biometrico e poi verificare se corrisponda o meno a una persona nota al sistema. Questa funzionalità si basa quindi sul confronto di un modello con una banca dati di modelli o campioni (riferimento); è detta anche identificazione 1:molti e, per esempio, può collegare a un volto un codice di prenotazione (cognome, nome) se si effettua il confronto con una banca dati di fotografie associate a nomi e cognomi, oppure comportare la possibilità di seguire una persona in mezzo a una folla, senza necessariamente creare il collegamento con l'identità civile della persona».

[25] Cfr. Comitato Europeo, Linee guida cit. 11ss.

[26] Sul punto, sia consentito il richiamo alla nota 3 di cui *supra*.

[27] In questo senso, Mobilio, *Tecnologie* cit. 139ss. Si è evidenziato che «La costruzione di enormi database di immagini, infatti, non implica l'applicazione del regime sui dati biometrici, sebbene una vasta disponibilità di immagini, grazie anche – come visto in precedenza – all'ampia diffusione di TRF a basso costo e allo sviluppo di tecniche di "big data analytics" sempre più raffinate, consenta molto facilmente di operare una identificazione a partire da semplici fotografie digitali».

Esemplificativa in tal senso appare la decisione assunta dal Garante italiano per la protezione dei dati personali nel noto caso Clearview[28], il quale ha rilevato la sussistenza di un trattamento biometrico allorquando l'attività posta in essere non si limiti ad una mera raccolta di immagini, nella fattispecie attraverso tecniche di "web scraping", ma si sostanzi in una vera e propria elaborazione di informazioni sensibili ovvero in una indicizzazione mediante "hashing". In altre parole, «le immagini raffiguranti volti di persone vengono sottoposte ad ulteriori operazioni di trattamento (rappresentazione vettoriale) che trasformano l'immagine comune (dato personale) in immagine facciale (dato biometrico)»[29].

Ciò che allora appare utile e necessario è distinguere il dato biometrico in quanto tale (ovvero il risultato del trattamento, finalizzato all'identificazione di un soggetto) dalla fonte dell'informazione medesima (la ripresa video, la fotografia, la registrazione).

Solo se l'obiettivo perseguito è quello di individuare univocamente una data persona fisica, a partire da caratteristiche irripetibili della stessa ed attraverso l'utilizzazione di specifici strumenti tecnici, allora potranno considerarsi i relativi dati quali informazioni sensibili *ex* articoli 4 e 9 del G.D.P.R[30].

3.- **Il problema del consenso "invisibile".**

La puntuale e rigorosa qualificazione dei dati personali elaborati dagli strumenti di riconoscimento facciale quali informazioni sensibili sottopone la relativa disciplina a regole rigide e quantomai stringenti ai fini della migliore tutela delle libertà individuali[31].

[28] J. Piemonte, V. Papakonstantinou, *Il caso Clearview AI: uno stress test per il Regolamento generale per la protezione dei dati e la proposta di Regolamento sull'intelligenza artificiale in relazione alle nuove sfide poste dal riconoscimento facciale*, in *Ciberspazio e diritto* 1(2023) 45ss.

[29] Ordinanza di ingiunzione nei confronti di Clearview AI, 10/02/2022, n. 50.

[30] In ambito nazionale, l'art. 2 *septies* del D.lgs. 101/2018 attua l'art. 9, par. 4 del G.D.P.R., prevedendo che il trattamento dei dati biometrici, genetici e relativi alla salute sia subordinato all'osservanza di misure di garanzia, stabilite dal Garante con provvedimento adottato con cadenza almeno biennale, a seguito di consultazione pubblica, tenendo in particolare considerazione, oltre alle linee guida, raccomandazioni e migliori prassi pubblicate dal Comitato europeo per la protezione dei dati, anche l'evoluzione tecnologica e scientifica del settore a cui tali misure sono rivolte, nonché l'interesse alla libera circolazione dei dati nel territorio europeo.

[31] Si fa qui riferimento alle regole imposte dal Reg. (UE) 2016/679, art. 9.

Invero, la giusta categorizzazione degli identificatori biometrici impone la necessaria applicazione di un livello di protezione particolarmente elevato, che consenta nella massima misura possibile di evitare rischi eccessivi per i diritti, sovente di natura fondamentale, degli interessati, primo fra tutti quello connesso all'autodeterminazione informativa degli utenti.

In ambito europeo, in assenza di una normativa armonizzata tesa a regolamentare lo specifico settore delle TRF, la disciplina appare plasmata sul G.D.P.R. e sull'AI ACT[32]. Tali informazioni, dunque, *in primis* risultano assoggettate alle disposizioni previste in tema di "personal data" ovvero al peculiare regime di "liceità"[33] delineato dall'art. 9 del G.D.P.R. La norma, imponendo un divieto generale di trattamento di dati sensibili[34], individua il consenso quale baluardo per la tutela, unitamente alle ulteriori basi giuridiche

[32] Reg. (UE) 13/06/2024, n. 1689, del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). La normativa, che rappresenta il primo tentativo a livello globale di regolamentare questa tecnologia emergente, si caratterizza per essere "risk-based", vale a dire che essa disciplina la materia mediante una classificazione dei sistemi di intelligenza artificiale (di seguito, IA) in base al livello di rischio associato al loro uso. Viene stabilita una distinzione tra sistemi a rischio «inaccettabile» (sistemi di IA che violano i diritti fondamentali o che sono utilizzati con modalità manipolative o ingiuste, come i "software" di sorveglianza di massa o i sistemi di IA che impiegano tecniche di "social scoring" da parte dei governi), «elevato» (vi rientrano i sistemi di IA utilizzati in ambiti critici come la sanità, i trasporti e la giustizia; tali sistemi devono soddisfare requisiti rigorosi in termini di trasparenza, "explainability", sicurezza e supervisione), «limitato» (per questa categoria è enfatizzato il requisito della trasparenza e vi rientrano, ad esempio, i "chatbot") o «minimo» (ad esempio: l'IA utilizzata in giochi, o per creare "playlist" musicali personalizzate; il "software" che automatizza compiti ripetitivi e di "routine" in contesti aziendali, come la gestione di fatture o la programmazione di appuntamenti; i sistemi che analizzano grandi set di dati per identificare tendenze di mercato e preferenze dei consumatori, senza prendere decisioni automatiche che hanno un impatto significativo sugli individui). Con l'AI Act, pur lasciandosi invariata la base giuridica di cui all'art. 114 T.F.U.E., sono stati introdotti una serie di principi etici che hanno dato alla normativa un'impostazione antropocentrica.

[33] Reg. (UE) 2016/679, art. 5.1, lett. a.

[34] Reg. (UE) 2016/679, art. 9.1: «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». La disposizione si pone, altresì, in continuità con la Convenzione 108+, *Convention for the protection of individuals with regard to the processing of personal data*, laddove all'art. 6 stabilisce che per il trattamento dei dati biometrici occorrono appropriate misure di salvaguardia stabilite dalla legge, che mettano al riparo dai rischi nei confronti degli interessi, diritti e libertà fondamentali del titolare dei dati, specialmente contro le discriminazioni.

ivi specificatamente individuate, quantomeno nel settore privato[35], degli identificatori biometrici[36]. Affinché l'utilizzo delle TRF possa dirsi legittimo, quindi, occorre che non solo vi sia una «manifestazione di volontà libera, specifica, 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»[37], ma che la stessa possa qualificarsi come «esplicita», scevra da eventuali pressioni o condizionamenti.

Nella materia in esame, tuttavia, proprio per le caratteristiche e la pervasività dei suddetti meccanismi, tale formula potrebbe rappresentare una regola declamatoria vuota o imperfetta, talvolta automatica[38], inidonea, cioè, ad orientare efficacemente l'interpretazione e l'applicazione delle norme nella ricerca di giuste tutele per le posizioni giuridiche dei singoli[39].

É evidente, infatti, che l'attività di elaborazione dei dati biometrici, attraverso l'impiego di tecnologie non sempre facilmente riconoscibili dagli utenti, rischia di porsi in contrasto con il diritto all'autodeterminazione, nella misura in cui il trattamento, eseguito senza che

[35] Con riguardo al trattamento dei dati per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali ad opera delle competenti autorità, ai sensi di quanto disposto dal considerando n. 35 della Dir. (UE) 27/04/2016, n. 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, «il consenso dell'interessato, quale definito nel Regolamento (UE) 2016/679, non dovrebbe costituire la base giuridica per il trattamento di dati personali da parte delle autorità competenti. Qualora sia tenuto ad adempiere un obbligo legale, l'interessato non è in grado di operare una scelta autenticamente libera, pertanto la sua reazione non potrebbe essere considerata una manifestazione di volontà libera. Ciò non dovrebbe impedire agli Stati membri di prevedere per legge che l'interessato possa acconsentire al trattamento dei propri dati personali ai fini della presente direttiva, ad esempio per test del DNA nell'ambito di indagini penali o per il monitoraggio della sua ubicazione mediante dispositivo elettronico per l'esecuzione di sanzioni penali».

[36] Reg. (UE) 2016/679, art. 9.2 «Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: 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».

[37] Reg. (UE) 2016/679, artt. 7-8.

[38] M.L. Jones, E. Kaufman, E. Ederberg, *AI and the Ethics of Automating Consent*, in *IEEE Security & Privacy* 16.3 (2018) 64ss.

[39] In questi termini, S. Orlando, *Consenso al trattamento e liceità*, in *Persona e Mercato* 2 (2024) 340ss.

il soggetto possa dirsi effettivamente consapevole, non gli consente di poter decidere in autonomia in che modo le informazioni che lo riguardino siano acquisite e conservate[40].
In altre parole, in tale contesto, rivive con nuova forza la questione dell'accettazione[41], quale espressione degli interessi individuali[42].
Ciò si manifesta tanto con riguardo ai sistemi cd. "passivi" di riconoscimento facciale (ad esempio l'ingresso in una zona videosorvegliata), ove la raccolta dei dati, attesa la mancanza di interazione uomo-macchina, può prescindere dalla percezione del titolare degli stessi[43], ritenendosi – illecitamente – acquisito il consenso quasi per *facta concludentia* (il passaggio nell'area videosorvegliata); quanto con riferimento a quelli "interattivi", per i cui trattamenti, sebbene si realizzi in concreto una partecipazione più penetrante dell'utente, che esprime il proprio *placet*, andrà comunque verificata l'effettività dell'autorizzazione in tal senso prestata.
L'aver acconsentito ad una determinata informativa "privacy", come ormai assolutamente noto, non necessariamente sottintende la reale conoscenza circa il contenuto della stessa e le conseguenze da essa promananti.

[40] In particolare, nel settore pubblico, considerando lo squilibrio di poteri tra individui interessati dal trattamento e autorità pubbliche, il tradizionale e diffuso requisito del consenso potrebbe rivelarsi insufficiente: «legislators and decision makers have to lay down specific rules for biometric processing using facial recognition technologies for law enforcement purposes. These rules will ensure that such uses must be strictly necessary and proportionate to these purposes and prescribe the necessary safeguards to be provided». Nell'ambito dei settori privatistici, invece, «The use of facial recognition technologies by private entities, except for private entities authorised to carry out similar tasks as public authorities, requires according to Article 5 of Convention 108+ the explicit, specific, free and informed consent of data subjects whose biometric data is processed». In argomento Di Matteo, *La riservatezza* cit. 89ss.

[41] Reg. (UE) 2016/679, art. 6.1: «Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità». In argomento, P. Stanzione, *La libertà e il suo valore*¸ in Cerrina Feroni (cur.), *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, Bologna 2024, 149ss.; G. Cerrina Feroni, *I dati personali come oggetto di un diritto fondamentale*, in P. Stanzione (cur.), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino 2022, 61ss.; V. Ricciuto, *Consenso al trattamento e contratto*, in *Pers. merc.* (2024) 14ss.; Id., L*'equivoco della privacy. Persona vs dato personale*, Napoli 2022.

[42] P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. Pardolesi (cur.), D*iritto alla riservatezza e circolazione dei dati personali*, Milano 2003, 395ss.; D. Imbruglia, *Le presunzioni delle macchine e il consenso dell'interessato*, in *Riv. trim. dir. proc. civ*. (2023) 921 ss.

[43] Mobilio, *Tecnologie* cit. 147ss.

Da qui le proposte di regolazione, dirette a risolvere in via successiva e rimediale i possibili usi distorti dei "personal data", vietando quelli illegittimi oppure rafforzando il potere di controllo e di sfruttamento economico degli stessi[44].

In particolare, da ultimo l'IA ACT ha provveduto a definire i casi di utilizzo di sistemi di intelligenza artificiale dediti alla «identificazione biometrica», intesa come «il riconoscimento automatico di caratteristiche fisiche, fisiologiche e comportamentali di una persona, quali il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti, allo scopo di determinare l'identità di una persona confrontando i suoi dati biometrici con quelli di altri individui memorizzati in una banca dati di riferimento, indipendentemente dal fatto che la persona abbia fornito il proprio consenso»[45].

Il Regolamento n. 1689/2024, dunque, introduce un divieto generale sull'impiego di meccanismi di riconoscimento facciale cd. in tempo reale – ossia quelli in cui l'autenticazione avviene senza ritardi significativi – per la sorveglianza di massa in spazi pubblici, salvo eccezioni in casi all'uopo individuati[46].

Al contempo, la norma classifica i sistemi di identificazione biometrica cd. a distanza, come "high-risk systems", richiedendo una valutazione rigorosa da parte delle autorità competenti ai fini del rilascio dell'autorizzazione al rispettivo sfruttamento. Trattasi di verifiche finalizzate a valutarne l'accuratezza e l'affidabilità, nonché a garantire la sicurezza dei dati acquisiti ovvero a minimizzare i rischi di discriminazione[47].

Sebbene per tali settori, quindi, alle tutele stabilite dal G.D.P.R. si sommino tutte quelle non basate sul consenso, stabilite dall'IA ACT per i sistemi ad alto rischio, per le categorie

[44] In questi termini Mobilio, *Tecnologie* cit. 153.

[45] Reg. (UE) 2024/1689, considerando n. 15.

[46] Reg. (UE) 2024/1689, art. 5. Tra le eccezioni previste dalla norma rilevano: l'utilizzo delle TRF per la ricerca di persone scomparse, prevenzione di reati gravi e l'identificazione di persone in situazioni di vulnerabilità.

[47] Reg. (UE) 2024/1689, artt. 6ss.

escluse, destinate ad esempio alla verifica biometrica, continuerà a trovare applicazione l'impianto giuridico preesistente[48].

Anche in prospettiva comparata, in particolare con riferimento alla legislazione degli Stati Uniti, emerge l'assenza di un quadro uniforme in materia, atto a tutelare in maniera cogente il fenomeno ed il sotteso diritto di "self determination".

Se, infatti, manca a livello federale una normativa organica[49], risultando l'utilizzo di tali tecnologie affidato principalmente a singole agenzie federali, come la Federal Trade Commission (FTC), a livello statale, invece, la regolamentazione delle TRF assume una posizione sempre più incisiva.

Ne è un chiaro esempio il Biometric Information Privacy Act ("BIPA"), adottato dallo stato dell'Illinois già a partire dal 2008, al fine di definire "standards" per la gestione delle informazioni biometriche dei consumatori da parte di enti privati, esercitanti attività lucrativa. In tal senso è imposto un esplicito obbligo, per l'azienda medesima, di notifica ed acquisizione dell'assenso dell'interessato, secondo precipui requisiti di trasparenza: «No private entity may collect, capture, purchase, receive through trade, or otherwise

[48] Cfr. F. Mollo, *Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*, in *Federalismi* 28 (2024) 91ss; P. Stanzione, *La via europea all'intelligenza artificiale*, in *Iustitia*, 1-2 (2022) 85ss.

[49] Evidenzia, in particolare, Orlando, La regolamentazione cit. 1121ss., che «sarebbe quantomeno ingeneroso sottovalutare il dibattito esistente a livello federale». Occorre, infatti, tenere debitamente in considerazione le proposte formulate in materia con riferimento al «Facial Recognition and Biometric Technology Moratorium Act, presentato al Congresso nel 2021 e poi nuovamente nel 2023, relativo appunto alle TRF nello specifico, intese come categoria speciale di sorveglianza biometrica bisognosa di autonoma disciplina. Il testo è dedicato soltanto all'utilizzo "pubblico" delle TRF da parte del Governo federale e delle amministrazioni statali e locali. Dopo aver fornito una definizione di "riconoscimento facciale", la proposta immagina un divieto generalizzato di utilizzo di sistemi di sorveglianza biometrica, ad eccezioni di ipotesi che il Congresso è chiamato a stabilire con successivo atto. In aggiunta, si impone agli Stati membri di uniformare la disciplina statale a quella federale, salvo possibilità di istituire regimi ulteriormente restrittivi. Sempre con riguardo al "law enforcement", un'altra proposta di legge più articolata – denominata "Facial Recognition Act of 2022"– opta come regola generale per un regime autorizzatorio: sarà l'autorità giudiziaria a consentire per non più di sette giorni l'utilizzo del sistema alle forze dell'ordine, le quali nella richiesta dovranno indicare o descrivere la persona che intendono identificare e motivare sulla probabilità che il sospettato abbia commesso un "serious violent felony". Non sarebbe richiesta invece autorizzazione per l'identificazione (rectius: per "assistere" l'identificazione) di vittime di reato o per i soggetti legalmente arrestati, né laddove il "prosecutor" valuti sussistente una emergenza, salvo convalida da parte dell'autorità giudiziaria entro dodici ore. Al di fuori di questo regime, restano espressamente vietati utilizzi volti ad agevolare l'applicazione della normativa sulla immigrazione, così come l'utilizzo di "body camera" se droni e qualsiasi forma di "face surveillance"».

obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative»[50]. La legge, inoltre, espressamente vieta agli operatori del settore di trarre profitto in altro modo dalle caratteristiche fisiche e morfologiche degli utenti, consentendo loro, nel caso di abusi o di usi distorti, di adire le Corti competenti per la migliore tutela dei propri diritti[51].

Ancora, il Texas Capture Or Use Of Biometric Identifier Act del 2009 ("CUBI") proibisce il trattamento degli identificatori biometrici di un individuo (scansione della retina o dell'iride, impronta digitale, impronta vocale o registrazione della geometria della mano o del viso) per uno scopo commerciale, a meno che non siano ottemperati specifici obblighi informativi nei propri confronti ed ottenuto il rispettivo consenso esplicito[52]. Con alcune eccezioni, la norma limita anche la vendita, la locazione o la divulgazione di tali informazioni e richiede che esse vengano distrutte entro un lasso di tempo ragionevole.

Trattasi, chiaramente, di disposizioni orientate ad individuare forme di regolamentazione delle TRF in atti di "hard law", che impongono ai legislatori di stabilire un bilanciamento a priori tra rischi e benefici[53].

4.- **Quali sfide per la tutela dei diritti fondamentali?**

[50] Illinois Biometric Information Privacy Act (BIPA) of 2008, 740 ILCS 14, sec. 15.

[51] Illinois Biometric Information Privacy Act (BIPA) of 2008, 740 ILCS 14, sec. 20.

[52] Texas Business and Commerce Code, tit. 11(A), sec. 503.001: «A person may not capture a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2) receives the individual's consent to capture the biometric identifier».

[53] In tal senso Orlando, *La regolamentazione* cit. 1126ss.

Ebbene, diviene imperativo delineare quali siano le libertà fondamentali[54] che queste tecnologie possono potenzialmente intaccare e le modalità con cui tale intrusione possa concretizzarsi, penetrando nei meandri più delicati della sfera individuale e compromettendo i diritti inalienabili di ciascuno[55].

Nello specifico, esse minacciano di sovvertire la percezione stessa di ciò che significa essere riconosciuti come soggetti unici ed irripetibili. L'identità[56], nelle sue molteplici

[54]Il ricorso alle TRF implica una interferenza con la libertà personale, verso la quale la libertà di manifestazione del pensiero possiede una dimensione ed una funzione strutturale, entrambe espressamente contemplate dalla Carta costituzionale. La sorveglianza di massa, invero, può generare un effetto dissuasivo dei comportamenti umani, noto come "chilling effect". La consapevolezza di essere costantemente osservati potrebbe condizionare l'autonomia di movimento, di espressione e di associazione. Significative, in tal senso, appaiono le pronunce della Corte europea dei diritti dell'uomo (CEDU). Più precisamente, nel caso Glukhin c. Russia , la Corte si è pronunciata per la prima volta su simili tecnologie evidenziandone i rischi derivanti da sistemi di sorveglianza non trasparenti e potenzialmente abusivi. Con un linguaggio perentorio, i giudici hanno ribadito che nessuna finalità, neanche quella della sicurezza collettiva, può giustificare una compressione sproporzionata del diritto al rispetto della propria vita privata ex articolo 8 CEDU e della libertà di manifestare il proprio pensiero ex articolo 10 CEDU, richiedendo che le TRF siano impiegate solo se legali, giustificate da un obiettivo legittimo necessario in una società democratica, proporzionato e adeguatamente motivato. Corte EDU, 4/07/2023, n. 1519/20. Inoltre, si legge in Council of Europe, Committee of Ministers, Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, 11/06/2013, come le forme di sorveglianza di massa «can have a chilling effect on citizen participation in social, cultural and political life and, in the longer term, could have damaging effects on democracy». Più ampiamente, cfr. N.M. Richards, *The Dangers of Surveillance*, in *Harvard Law Review* 2 (2013) 146ss.

[55] Cfr. S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari 1997, 165; Id., *Tecnologie e diritti*, Bologna 1995; G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto* 2 (2019) 200ss.; T.E. Frosini, *Il costituzionalismo nella società tecnologica*, in *Liber Amicorum per Pasquale Costanzo*, Genova 2020; F. Pizzetti, *Società digitale, perché il Gdpr è presidio di diritti fondamentali*, in *https://www.agendadigitale.eu*.

[56] Come è noto, il diritto all'identità personale trova le sue radici nell'ordinamento italiano attraverso una complessa elaborazione dottrinale e giurisprudenziale. Da una concezione originariamente legata alla tutela dei segni distintivi, esso si è progressivamente evoluto fino a essere definito quale «diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo». Tale diritto riveste, dunque, un'immediata rilevanza costituzionale, in quanto strettamente connesso sia al pieno sviluppo della persona, sia all'interesse della collettività nel riconoscere e comprendere l'identità autentica dei suoi membri. Si veda, Corte Cost., 24/01/1994, n. 13, nella quale si assiste ad una contrapposizione tra due tesi: quella che individua quale norma di copertura l'art. 2 Cost. e quella che, invece, fa ricorso alla tutela della propria dignità contro rappresentazioni false e disonoranti, individuando il fondamento nel combinato disposto *ex* artt. 3 e 21 Cost. Cfr. G. Finocchiaro, *Identità personale (diritto alla)*, in *Dig. disc. priv., sez. civ.* 5 (2010) 726, che inquadra l'identità personale come «l'immagine sociale di un soggetto quale oggettivamente rilevabile», intesa né come l'immagine che il

declinazioni, inclusa quella digitale[57], emersa con il crescente radicarsi delle attività svolte nel mondo virtuale, rappresenta un'espressione tangibile della dignità umana che appare minacciata dalla progressiva trasformazione del volto – specchio dell'essere – in un dato biometrico manipolabile, archiviabile e spesso esposto a potenziali abusi (*id est* ai cyber-attacchi)[58]. Ci si riferisce alla pericolosa decontestualizzazione dell'informazione rispetto alla complessità integrale della persona, destinata a raggiungere il suo massimo compimento nelle tecniche avanzate di profilazione. Questo processo conduce ad una vera e propria funzionalizzazione dell'individuo, ridotto ad un frammento estrapolato dal suo contesto globale ed utilizzato per scopi specifici e predeterminati. Da questa rappresentazione incompleta scaturiscono decisioni che spaziano dall'abilitare o negare l'accesso a beni e servizi, alla selezione e limitazione delle informazioni rese visibili ad un utente, sino alla possibilità di essere oggetto di discriminazioni o sottoposto a particolari forme di controllo da parte delle autorità pubbliche[59].

Le criticità aumentano laddove tali informazioni vengano utilizzate per finalità non comprese, né tanto meno autorizzate, ponendosi in tal senso un'esigenza di tutela del diritto alla riservatezza, nella sua moderna accezione di diritto alla "privacy"[60]. Invero,

soggetto ha di sé (verità personale), né come l'insieme dei dati oggettivi riferibili al soggetto (verità storica), ma quale sintesi costituita dall'immagine, socialmente mediata o oggettivata, del soggetto stesso.

[57] L'identità digitale può essere intesa come sinonimo di identità "in rete", in accordo anche con il significato fatto proprio dalla «Dichiarazione dei diritti in Internet» del 28 luglio 2015, oppure come «la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale», alla stregua di quanto stabilito dal Codice dell'amministrazione digitale. Si veda per un approfondimento G. Resta, *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica* 3 (2017) 514 ss.; I. Tardia, *L'identità digitale tra memoria ed oblio*, Napoli 2017, 66 ss.

[58] Il furto o l'indebito utilizzo dell'identità digitale trovano adesso sanzione penale a seguito dell'introduzione di una nuova circostanza aggravante al reato di frode informatica *ex* art. 640 *ter* c.p.: il bene protetto dalla norma, tuttavia, risulta essere il patrimonio e non l'identità in sé, per cui occorre necessariamente procurare un «ingiusto profitto» per integrare tale fattispecie.

[59] Cfr. Comitato Nazionale per la Bioetica, L'identificazione del corpo umano: profili bioetici della biometria, 26/11/2010.

[60] Corte Cost., 11/07/1991, n. 366, afferma che il diritto alla riservatezza è stato qualificato quale «manifestazione del diritto fondamentale all'intangibilità della sfera privata» e attinente alla tutela della vita degli individui nei suoi molteplici aspetti, che trova riferimento negli artt. 2, 14, 15 Cost., oltre che in varie norme dell'UE e convenzionali, quali gli artt. 7 e 8 della CDFUE e l'art. 8 della CEDU. Sul tema, A. Cerri, *Riservatezza (diritto alla). Diritto costituzionale*, in *Enc. giur.* 17 (1995) 3ss., il quale sottolinea che,

non è solo l'accesso non consentito ai dati personali ad essere lesivo, ma anche e soprattutto il modo in cui essi sono elaborati e reinterpretati senza che il titolare abbia alcun governo sul processo.

Attraverso questa prospettiva, allora, emerge un cambiamento paradigmatico: dalla concezione "negativa" della riservatezza, intesa come diritto ad escludere interferenze esterne nella propria sfera personale, si evolve verso una visione "positiva" che assegna all'individuo il controllo sull'insieme dei dati che rappresentano il riflesso della sua esistenza nella società digitale[61].

La frammentazione dell'identificatore biometrico e la sua riduzione ad uno strumento per scopi predeterminati comportano una perdita del controllo sulla propria immagine, privando il soggetto della possibilità di decidere come e in quale misura rendersi riconoscibile agli altri. In ultima analisi, la sovrapposizione tra la decontestualizzazione di tali informazioni e l'indebolimento del diritto alla "privacy" configura una nuova forma di controllo, che spoglia la persona della sua capacità di autodeterminarsi nella società digitale, restituendo una libertà apparente priva di autentica protezione[62].

Alla luce della pervasività delle nuove tecnologie la cui incidenza travalica i confini delle libertà e dei diritti fondamentali degli individui, quindi, non è possibile prescindere dalla necessità imperiosa di operare un bilanciamento ponderato tra i molteplici valori in gioco.

---

se si volesse operare una assimilazione tra riservatezza e "privacy", occorrerebbe fare riferimento ad una "costellazione di diritti" accomunati non da caratteri strutturali o formali, quanto da una matrice ideale di rifiuto da intrusioni in una sfera riconosciuta come propria della persona e della sua spontanea socialità, e dunque a "diritti" alla riservatezza che attingono al "pieno sviluppo della persona"; S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. Crit. del Dir. Priv.*, 15 (1997) 590ss.; G. Busia, *Riservatezza (diritto alla)*, in *Digesto delle discipline pubblicistiche*, Torino 2000; G. Martinico, *Art. 7. Rispetto della vita privata e della vita familiare*, in *Carta dei diritti fondamentali dell'Unione europea*, Milano 2017, 119ss.; A. Pace, M. Manetti, *Commento all'art. 21*, in G. Branca (cur.), *Commentario della Costituzione*, Bologna - Roma 2006.

[61] Per un approfondimento si veda, S. Rodotà, *Tecnologie e diritti*, Bologna 1995; Id., *Persona* cit. 588ss.; Id., *Il diritto di avere diritti*, Bari 2012; L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli 2016; C. Colapietro, A. Iannuzzi, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano, C. Colapietro (curr.), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli 2017, 87ss.; European Commission, Communication "A Digital Single Market Strategy for Europe" SWD(2015) 100 final, 6/05/2015.

[62] Cfr. S. Monteleone, *Privacy, data protection e identità elettronica. Tra rapidi sviluppi della tecnologia e nuovo approccio europeo*, in M. Villone (cur.), *Nuovi mezzi di comunicazione e identità. Omologazione o diversità?*, Roma 2021, 533ss.; Perri, *Sorveglianza* cit. 25ss.

Tuttavia, tale giudizio, nella sua applicazione concreta, sembra manifestarsi in modo alquanto asimmetrico, con una netta prevalenza delle esigenze di natura pubblicistica. In particolare, quando il legislatore, europeo e nazionale, opera scelte normative che favoriscono le istanze collettive, sacrificando talvolta la protezione dei diritti individuali, determina un trattamento normativo differenziato e, in certi casi, problematico. Il settore pubblico, infatti, gode di una sorta di "autorizzazione implicita" per l'utilizzo delle TRF, laddove scopi di sicurezza sociale, di prevenzione e di perseguimento dei reati legittimano il trattamento dei dati personali senza necessità di acquisire il consenso del soggetto interessato. In questi casi, allora, simili finalità istituzionali divengono fondamento sufficiente ed autonomo per la liceità del trattamento, con una sospensione *de facto* della partecipazione attiva dell'individuo[63].

Al contrario, nel settore privato, la situazione si complica notevolmente laddove l'assenso dell'interessato diventa il pilastro centrale della protezione del diritto alla "privacy". Tuttavia, come evidenziato, questa stessa condizione si rivela sempre più inadeguata ed inefficace di fronte alla rapida evoluzione delle tecnologie, come quelle di riconoscimento facciale, che minano la libertà di autodeterminazione dell'individuo.

[63] Sia consentito il richiamo alla nota 34 *supra*.

Abstract.- Le tecnologie di riconoscimento facciale, alimentate spesso da algoritmi di intelligenza artificiale, rappresentano una delle applicazioni più avanzate, ma anche più controverse, nell'ambito dei dati biometrici. Il quadro normativo, attualmente vigente, sebbene tenti di regolamentare il fenomeno, allo stato rimane incompleto rispetto alla gestione complessiva delle informazioni in esame, specie se in considerazione delle vulnerabilità associate alla tutela delle libertà fondamentali. Emergono, infatti, con forza le criticità legate alla potenziale erosione della "privacy" ed ai rischi di sorveglianza di massa. Occorre, pertanto, invocare un approccio responsabile e consapevole, capace di garantire che queste tecnologie, potenti e pervasive, possano essere strumenti al servizio del bene comune piuttosto che minacce per le libertà individuali.

Facial recognition technologies, often powered by artificial intelligence algorithms, represent one of the most advanced yet controversial applications in the field of biometric data. The current regulatory framework, while attempting to govern the phenomenon, remains incomplete in addressing the overall management of the information under consideration, especially given the vulnerabilities associated with safeguarding fundamental freedoms. Indeed, significant concerns arise regarding the potential erosion of privacy and the risks of mass surveillance. It is therefore essential to advocate for a responsible and informed approach, capable of ensuring that these powerful and pervasive technologies serve the common good rather than becoming threats to individual liberties.