

CIRO MARIA RUOCCO, LUCA ESPOSITO

OMBRE DIGITALI DELL'IDENTITÀ. BIOMETRIA, PROFILAZIONE E POTERE DEL TRATTAMENTO AUTOMATIZZATO

SOMMARIO: 1. Il dato biometrico come dato personale e particolare nel paradigma europeo della protezione. — 2. Dati biometrici e profilazione: il confine sottile tra identità e sorveglianza nell'era dell'intelligenza artificiale. — 3. Dai tratti del volto ai tratti dell'identità: il passaggio dalla biometria alla profilazione. — 4. Biometria e vulnerabilità algoritmica: quando il corpo diventa fragilità esposta. — 5. Biometria pubblica, mutamento di finalità e dovere di responsabilizzazione: le sfide sistemiche del trattamento. — 6. L'illusione dell'anonimizzazione e il rischio persistente di re-identificazione nei dati biometrici. — 7. Riflessioni conclusive. Restare liberi, nonostante il dato.

I. IL DATO BIOMETRICO COME DATO PERSONALE E PARTICOLARE NEL PARADIGMA EUROPEO DELLA PROTEZIONE.

L'analisi giuridica in tema di dati biometrici non può che prendere le mosse da una riflessione preliminare sulla loro esatta qualificazione normativa, interrogandosi circa la possibilità — e i limiti — di una loro riconduzione nell'alveo della più ampia categoria dei dati personali.

Siffatta questione non è di mero inquadramento teorico, ma assume una rilevanza sostanziale, poiché la qualificazione di un'informazione come dato personale implica l'applicabilità, com'è ampiamente noto, della normativa in materia di protezione dei dati, con tutte le tutele e i vincoli che ne derivano. Il Regolamento (UE) 2016/679 (GDPR) fornisce una definizione estremamente ampia di dato personale, intendendolo come « *qualsiasi informazione riguardante una persona fisica identificata o identificabile* »¹. L'identificabilità può avvenire sia in maniera di-

* Il presente saggio, pur se unitamente concepito dai due Autori, deve essere così attribuito nelle sue singole parti: §§ 1, 3 e 5 a Ciro Maria Ruocco; §§ 2, 4 e 6 a Luca Esposito, mentre il § 7 è comune ad entrambi gli Autori.

¹ La nota definizione di “dato personale” è strutturalmente occlusa nell'alveo dell'art. 4 n.1 del GDPR, che testualmente statuisce: « *Qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera iden-*

retta, attraverso elementi univoci come il nome o un numero identificativo, sia in modo indiretto, mediante riferimenti a dati relativi all'ubicazione, identificatori *online* o qualsiasi caratteristica che consenta di risalire all'identità del soggetto ².

Questa impostazione, già presente nella Direttiva 95/46/CE, dimostra la volontà del legislatore europeo di adottare una nozione onnicomprensiva ³, in grado di adattarsi alle evoluzioni

tificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale ». Nel contesto di un sistema giuridico che ha ormai eletto la protezione dei dati personali a condizione essenziale per la tutela della dignità umana, l'art. 4, n. 1 del GDPR rappresenta, dunque, il nucleo semantico primigenio da cui si dirama l'intero edificio della normativa europea in materia. È nella definizione di dato personale che si radica la *ratio* del Regolamento: proteggere l'individuo nel suo essere e nel suo manifestarsi attraverso le tracce informative che lo rendono riconoscibile nel mondo digitale. Il legislatore europeo, in questa disposizione, adotta una nozione estesa e dinamica di dato personale, fondata su due assi interpretativi centrali: da un lato, la riferibilità dell'informazione a una persona fisica (criterio soggettivo); dall'altro, la idoneità all'identificazione, anche indiretta, dell'interessato (criterio oggettivo). Non è dunque necessario che un'informazione identifi-
fichi esplicitamente un individuo, come accade con un nome o un numero di passaporto: è sufficiente che essa, isolatamente o per correlazione con altri dati, consenta una reidentificazione. Questa apertura concettuale è coerente con la realtà tecnologica contemporanea, in cui frammenti di informazione — apparentemente innocui — possono essere aggregati da sistemi automatici di elaborazione per ricostruire profili identitari con elevata precisione. Il riferimento a "qualsiasi informazione" mostra, inoltre, l'intento del legislatore di non adottare un elenco tassativo, bensì una formula aperta, capace di adattarsi all'evoluzione dei contesti e delle tecnologie. Così, accanto agli identificativi classici (nome, numero di documento), troviamo elementi contestuali e relazionali (dati di localizzazione, identificatori *online*), ma anche attributi più profondi dell'identità personale, che spaziano dal corpo alla mente, dall'economia alla

cultura. Questa elencazione — solo apparentemente descrittiva — assume una funzione strutturale nella logica del GDPR, poiché prepara il terreno per la distinzione tra dati ordinari e « *categorie particolari di dati* » (art. 9), come i dati genetici, biometrici, relativi alla salute o alla vita sessuale, che esigono tutele rafforzate. Va poi sottolineato come la nozione di identificabilità assuma una connotazione relativa, e non assoluta: essa dipende dal contesto, dai mezzi ragionevolmente utilizzabili dal titolare del trattamento o da terzi per giungere all'identificazione. Questo approccio contestuale comporta che anche informazioni apparentemente anonime possano, in certi casi, rientrare nell'ambito applicativo del GDPR se esiste un rischio concreto di reidentificazione. Infine, questa definizione è lo snodo da cui dipende l'applicabilità stessa del Regolamento: se un'informazione non rientra nel concetto di dato personale, essa sfugge all'intero impianto protettivo del GDPR. Per questo motivo, la nozione ha un valore sistemico ed è oggetto di un'interpretazione evolutiva, che non può mai prescindere dal principio fondamentale della centralità della persona umana, secondo la visione ormai matura di un "diritto alla protezione dei dati" non più ancillare alla *privacy*, ma strutturalmente autonomo e volto a garantire l'autodeterminazione informativa dell'individuo.

² Una parte autorevole della dottrina italiana ha partecipato attivamente alla costruzione teorica del nucleo normativo di riferimento dei diritti della personalità, conferendogli struttura e sistematicità. Senza alcuna pretesa di esaustività, si veda, *ex multis*, D. MESSINETTI, voce « *Personalità (diritti della)* », in *Enc. dir.*, Milano 1983, XXXIII, pp. 355 ss.; P. RESCIGNO, voce « *Personalità (diritti della)* », in *Enc. giur. Treccani*, Roma, 1990, XXIII, pp. 2 ss.; V. ZENO-ZENCOVICI, voce « *Personalità (diritti della)* », in *Digesto civ.*, Torino, 1995, XIII, pp. 430 ss.

³ In questi termini, sull'analisi circa le scelte compiute dall'Unione Europea, anche in relazione al più ampio tema del trasferimento transfrontaliero dei dati, si veda

tecnologiche e alle nuove forme di trattamento dei dati ⁴. La stessa logica è rintracciabile nella definizione di dato biometrico, anch'essa delineata con un'impostazione volutamente descrittiva e non legata a specifiche tecnologie ⁵.

L'art. 4, n. 14 del GDPR definisce questi ultimi come « *dati personali ottenuti da un trattamento tecnico specifico relativi alle*

quanto evidenziato da S. SICA - V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in G. Resta - V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, pp. 137 ss. e spec. 138, ove, testualmente si afferma che: « *La scelta di policy dell'Unione, sotto questo profilo, è stata quella di porsi quale modello forte di tutela della riservatezza, imponendo a qualunque esportatore di dati personali di origine comunitaria di confrontarsi con lo schema normativo europeo, garantendo alle informazioni in transito un livello di tutela particolarmente elevato, modellato appunto sul paradigma della direttiva 95/46/CE* ».

⁴ Il progresso tecnologico, soprattutto nell'ambito delle scienze della vita e dell'intelligenza artificiale, ha spinto il diritto a misurarsi con nuove forme di informazione personale che superano le tradizionali categorie normative. Se in una prima fase l'attenzione del legislatore e della dottrina si è concentrata sui dati genetici, in quanto portatori di una struttura identitaria biologica profonda e immutabile, l'evoluzione tecnologica ha successivamente evidenziato la centralità dei dati biometrici, come elemento chiave nei sistemi di identificazione, autenticazione e profilazione. Si assiste così a una trasmutazione dell'interesse giuridico: dalla mappatura statica del genoma alla lettura dinamica dei tratti fisiologici e comportamentali, entrambi accomunati da un medesimo rischio di reificazione dell'identità personale e di sorveglianza pervasiva. Per un'accurata ricostruzione sull'evoluzione che la tecnologia ha determinato in relazione ai dati genetici si veda V. D'ANTONIO, *I dati genetici*, in F. Cardarelli - S. Sica - V. Zeno-Zencovich (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, pp. 337 ss.; Id., *Biometria, dati genetici e privacy: profili giuridici*, Salerno, 2004, *passim*. Più precipuamente — per l'Autore — con l'avanzare delle scienze biologiche e l'ampliarsi delle possibilità offerte dalla genetica, anche il diritto alla riservatezza ha conosciuto un'evoluzione significativa, tale da portare progressivamente all'elaborazione del concetto di "dato gene-

tico" come categoria giuridica autonoma. La riflessione si è subito concentrata sui profili critici legati al trattamento di tali informazioni, ponendo interrogativi sulla loro definizione, sulla loro gestione e, soprattutto, sulla titolarità dei relativi diritti. Da questo dibattito è emersa l'idea di una "privacy genetica", intesa come facoltà dell'individuo di controllare la circolazione delle informazioni più intime e strutturali del proprio patrimonio biologico. A questa traiettoria si è progressivamente affiancata, in linea con i mutamenti tecnologici e informatici, la rilevanza crescente dei dati biometrici, che, pur distinti da quelli genetici per natura e funzione, condividono con essi la capacità di svelare dimensioni identitarie profonde. Tali dati si distinguono, in particolare, per la loro unicità e per l'elevato potenziale identificativo, in quanto derivano, notoriamente, da caratteristiche fisiche o comportamentali non replicabili, che permettono di ricondurre in modo certo un'informazione ad un solo ed unico soggetto. In questa prospettiva, si assiste a un'evoluzione del diritto alla riservatezza, che si espande per includere nuove forme di espressione dell'identità personale, sempre più vulnerabili in ragione della pervasività tecnologica.

⁵ Le questioni legate alla biometria, oltre a rappresentare un nodo cruciale nell'agenda normativa dell'Unione Europea, si impongono progressivamente nel discorso pubblico, suscitando reazioni contrastanti. Da un lato, emergono preoccupazioni che evocano scenari di sorveglianza pervasiva, sollevando il timore di un controllo sociale diffuso; dall'altro, si riconosce la possibilità che tali strumenti, se disciplinati con adeguate garanzie, possano apportare benefici rilevanti in molteplici settori. Un aspetto non trascurabile riguarda la tendenza, spesso sottovalutata, con cui gli utenti si interfacciano con queste tecnologie, talvolta senza la piena consapevolezza delle implicazioni derivanti dalla condivisione dei propri dati biometrici. Emblematico è il caso dei dispositivi indossabili, i c.d. *wearable*, che rilevano parametri fisiologici e comportamentali — dai battiti cardiaci alla qualità del sonno — accumulando una mole di informazioni che, se non adeguatamente pro-

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 »⁶. La definizione non si limita a elencare esempi di dati biometrici, ma pone l'accento sulla loro funzione identificativa, evidenziando il ruolo della tecnologia nella loro elaborazione. Se l'appartenenza dei dati biometrici alla categoria dei dati personali appare evidente⁷, è altresì necessario considerare il loro inserimento nell'ambito dei dati particolari, soggetti a un regime di tutela rafforzato ai sensi dell'art. 9, par. 1 del GDPR⁸. La norma stabilisce un principio generale di divieto nel trattamento di determinate tipologie di dati, tra cui quelli biometrici quando utilizzati per iden-

tetta, rischia di alimentare pratiche di profilazione sempre più pervasiva. La riflessione su questi strumenti non può limitarsi a una valutazione dicotomica tra vantaggi e rischi, ma deve interrogarsi sulla sostenibilità di un modello tecnologico in cui il confine tra innovazione e sorveglianza si fa sempre più sottile. Cfr. E. GERMANI - L. FEROLA, *Il wearable computing e gli orizzonti futuri della privacy*, in questa *Rivista*, 2014, 1, pp. 75 ss.; V. ZENO-ZENCOVICH, *Ten legal perspectives on the "big data revolution"*, in *Conc. e merc.*, 2016, pp. 29 ss.; E.C. PALLONE, *"Internet of Things" e l'importanza del diritto alla "privacy" tra opportunità e rischi in Cib. e dir.*, 2016, Vol. 17, 55 (1/2), pp. 163 ss.; alternatively, per un approccio comparatistico, K. GUTIERREZ, *Privacy in Wearables: Innovation, Regulation, or Neither*, in *Hastings Sci. & Tech. Law Journal*, 2022, Vol. 13, 1, pp. 21 ss.; N. CHAURIYE, *Wearable devices as admissible evidence: technology is killing our opportunities to lie*, in *Cath. U. J. L. & Tech.*, 2016, Vol. 24, 2, pp. 495 ss.; Z. TAKHSHID, *Wearable AI, Bystander Notice, and the Question of Privacy Frictions*, in *Boston University Law Review*, 2024, Vol. 104, pp. 101 ss.

⁶ Sterminata è la bibliografia di autorevolissima dottrina che si è espressa in relazione alla biometria. Senza alcuna pretesa di esaustività, sui dati biometrici si veda E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Padova, 2008, pp. 4 ss.; R. DUCATO, *I dati biometrici*, in V. Cnffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 1285 ss.; F. FONTANAROSA, *Dati biometrici e tutela della "privacy" tra divergenze giuridiche ed esigenze di unificazione*, in *Ann. dir. comp.*, 2019, III, pp. 807 ss.; G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *DPCE online*, 2019, 2, pp.

1108; A. IANNUZZI - F. FILOSA, *Il trattamento dei dati genetici e biometrici*, in *Dir. fond.*, 2019, pp. 24; T. SICA, *Dati biometrici, tutela del singolo e opportunità di mercato*, in *Rivista di Diritti Comparati*, 2022, 3, pp. 965 ss.; A.C. NAZZARO, *La tutela dei dati biometrici tra GDPR e AI ACT*, in *European Journal of Privacy Law & Technologies (EJPLT)*, 2024, 2, pp. 2 ss.

⁷ La riconducibilità dei dati biometrici alla più ampia categoria dei dati personali non necessita di particolari sforzi interpretativi. Si tratta, in effetti, di una relazione definitoria che emerge con chiarezza dalla stessa struttura concettuale del GDPR, ove i dati biometrici sono descritti come una sottocategoria di dati personali, caratterizzata da una specifica potenzialità identificativa. Questa lettura è confermata anche dall'EDPB, che nelle Linee guida 3/2019, al par. 76, individua proprio nella capacità di permettere l'identificazione univoca dell'interessato uno degli elementi centrali per qualificare un trattamento come biometrico. È dunque nel rapporto tra trattamento tecnico specifico, caratteristica personale e funzione identificativa che si gioca la qualificazione del dato biometrico, rendendone evidente l'inclusione nella disciplina generale di protezione dei dati, ancor prima che nella sua articolazione rafforzata ai sensi dell'art. 9 del Regolamento.

⁸ L'art. 9 del Regolamento (UE) 2016/679 sancisce, com'è noto, un generale divieto di trattamento dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dei dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona. Il tenore letterale della norma recita: « È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'ap-

tificare univocamente una persona fisica. Questa scelta normativa risponde alla necessità di garantire una protezione più elevata per le informazioni che, per loro natura, potrebbero esporre i soggetti interessati a rischi significativi, come discriminazioni, violazioni della *privacy* o utilizzi impropri a fini di sorveglianza ⁹.

L'inserimento dei dati biometrici tra i dati particolari impone quindi agli operatori l'adozione di misure più stringenti ¹⁰, limitando il trattamento a specifiche condizioni di liceità, come il consenso esplicito dell'interessato o la necessità del trattamento per motivi di interesse pubblico rilevante ¹¹. Inoltre, l'approccio del GDPR, improntato alla neutralità tecnologica ¹², consente di estendere la protezione anche a nuove forme di biometria che

partenenza 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 » (art. 9, par. 1 GDPR). La norma introduce, così, un regime giuridico differenziato rispetto al trattamento dei dati "comuni", fondato su un principio di eccezionalità e necessità del trattamento, subordinandone la liceità a specifiche condizioni tassativamente elencate nel paragrafo 2 dello stesso articolo. Tale disciplina rappresenta una delle massime espressioni dell'idea di "tutela rafforzata" delle libertà fondamentali in ambiente digitale, in cui il trattamento di dati biometrici non è semplicemente una questione di riservatezza, ma una forma profonda di interferenza potenziale con l'identità personale. Questa impostazione si inserisce coerentemente nella concezione secondo cui la protezione dei dati personali si configura come strumento di cittadinanza, che garantisce la possibilità di autodeterminazione informativa e il controllo del proprio corpo digitale, la cui manipolazione può incidere sulla dignità, sulla libertà e persino sulla non discriminazione. La particolare valenza identitaria dei dati biometrici, in quanto elementi che connettono direttamente l'identificabilità dell'individuo a tratti corporali e comportamentali, giustifica una vigilanza normativa rafforzata, volta a evitare derive che rischiano di comprimere lo spazio privato, fino a dissolverlo. Alla luce di tale assetto, il trattamento di dati biometrici deve ritenersi sempre vietato, salvo che ricorrano le specifiche deroghe di cui all'art. 9, par. 2, tra cui figurano il consenso esplicito dell'interessato (lett. a), le necessità di diritto del lavoro (lett. b), gli interessi vitali (lett. c), finalità di sanità pubblica (lett. i), o rilevanti motivi di interesse pubblico (lett. g). Tuttavia, anche in tali casi, il trattamento dovrà avvenire in

piena coerenza con i principi generali di necessità, proporzionalità, minimizzazione e responsabilizzazione, così come delineati agli artt. 5 e 24 del medesimo Regolamento.

⁹ Sulla sorveglianza di massa, segnatamente si veda G. GREENWALD, *No place to hide. Sotto controllo. Edward Snowden e la sorveglianza di massa*, Milano, 2014; S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; G. ZICCARDI, *Il controllo e la privacy delle attività informatiche del lavoratore sul luogo di lavoro*, in L. Pelliccioli (a cura di), *La privacy nell'età dell'informazione: concetti e problemi*, Colle di Val d'Elsa (SI), 2016, pp. 65 ss.; P. PERRI, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, in G. Ziccardi - P. Perri (collana diretta da), *Informatica giuridica*, Milano, 2020, pp. 85 ss.

¹⁰ Sull'adozione di misure stringenti nel trattamento dei dati algoritmici e sulle funzioni riservate alle Autorità Garanti è quanto mai opportuno il rinvio ad A. ZOPPINI, *Il ruolo e le funzioni delle authorities nel trattamento algoritmico dei dati*, in Aa.Vv., *Il trattamento algoritmico dei dati tra etica, diritto ed economia. Atti del 14° Convegno nazionale*, Napoli, 2020, pp. 291 ss.

¹¹ Sulle tematiche relative al consenso, tra le voci più autorevoli, appaiono significative le considerazioni di G. AUTORINO STANZIONE, *Ricerca scientifica, consenso, tutela della persona*, in G. Comandé - G. Ponzanelli (a cura di), *Scienza e diritto nel prisma del diritto comparato*, Torino, 2004, pp. 299 ss.

¹² Il GDPR adotta un approccio c.d. di "neutralità tecnologica", ossia non vincola l'applicazione delle proprie disposizioni a uno specifico strumento tecnico o a determinate soluzioni tecnologiche. Tale impostazione è esplicitamente riconducibile al considerando n. 15 del GDPR, il quale chiarisce che le norme sulla protezione dei dati

potrebbero emergere con l'evoluzione scientifica e tecnica, consolidando un modello di regolazione flessibile e adattabile ai progressi futuri¹³. L'inquadramento normativo dei dati biometrici si colloca, dunque, in un delicato equilibrio tra esigenze di identificazione, che trovano crescente applicazione nei settori della sicurezza, della sanità e delle transazioni digitali, e la

personali devono applicarsi a prescindere dalla tecnologia utilizzata per il trattamento, purché il trattamento stesso riguardi dati personali riferibili a una persona fisica identificata o identificabile. Questa scelta riflette una consapevolezza strutturale del legislatore europeo: in un ecosistema in costante evoluzione, ogni riferimento diretto a tecnologie contingenti rischierebbe di rendere rapidamente obsoleto il quadro normativo, minando l'effettività delle garanzie predisposte a tutela dell'individuo. Il principio di neutralità, dunque, assume un ruolo funzionale alla resilienza normativa rispetto all'innovazione, assicurando che gli obblighi imposti ai titolari del trattamento restino validi indipendentemente dal mezzo impiegato, sia esso analogico, digitale, automatizzato, decentralizzato o mediato dall'intelligenza artificiale. Nel contesto dei dati biometrici, questa impostazione risulta di particolare rilievo: ciò che rileva non è tanto la tecnologia in sé (ad esempio, il tipo di algoritmo, il sensore impiegato, la forma di vettorializzazione del volto), quanto il fatto che essa realizzi un trattamento tecnico specifico in grado di identificare univocamente una persona fisica. È in questa prospettiva che si coglie la modernità dell'impianto regolatorio europeo: non una normazione dei mezzi, ma una disciplina delle finalità e degli effetti del trattamento, nel rispetto dei principi di proporzionalità, necessità e minimizzazione. In tal senso, la neutralità tecnologica si configura anche come criterio ermeneutico: vincola l'interprete a valutare la liceità del trattamento non in base alla novità o sofisticazione dello strumento utilizzato, ma alla sua incidenza concreta sui diritti e le libertà dell'interessato. Ne deriva un modello di protezione che non insegue l'innovazione, ma la precede, ponendo presidi giuridici capaci di reggere l'urto delle trasformazioni digitali più radicali. È ampiamente trattato il tema della neutralità della rete in G. GIANNONE CODICIONE, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in questa Rivista, 2015, pp. 909 ss.; altresì, sulla *net-neutrality*, S. VIGLIAR - V. VARRIALE - G. GIANNONE CODICIONE, *Neutrality, data protection e crime preven-*

tion nelle comunicazioni elettroniche, in S. Sica - V. Zeno-Zencovich (a cura di), *Manuale di diritto dell'informazione e della comunicazione*, Padova, 2022, pp. 365 ss.

¹³ Prima di addentrarsi nello scenario futuristico che potrebbe derivare da nuove forme di dati biometrici e dalla biometria, è singolare, quanto opportuno, evidenziare una connessione concettualmente pregnante — da considerarsi quale antenato delle moderne pratiche biometriche in chiave comparatistica — al sistema introdotto nel 1882 da Alphonse Bertillon presso le carceri di Parigi. Si trattava di un metodo di identificazione fondato sulla rilevazione standardizzata di misure corporee (tra cui lunghezza del capo, dita e arti), integrate da fotografie segnaletiche frontali e laterali, nonché da annotazioni relative a tratti fisionomici peculiari. Tale sistema, noto come *bertillonage*, mirava a garantire l'individuazione certa dei recidivi attraverso un profilo antropometrico che, nelle intenzioni del suo ideatore, avrebbe dovuto essere irripetibile e stabile nel tempo. In un contesto storico privo di garanzie normative in materia di protezione dei dati personali, questa pratica venne percepita come uno strumento scientifico di razionalizzazione dell'identificazione penitenziaria, più che come una violazione della riservatezza individuale. La sua progressiva adozione da parte di numerose polizie europee e statunitensi segnala l'ampia diffusione dell'idea secondo cui le caratteristiche corporee dell'individuo potessero divenire oggetto di trattamento sistematico per finalità di riconoscimento — anticipando, sotto certi profili, l'attuale concezione del dato biometrico quale elemento identificativo per eccellenza. Tuttavia, il metodo si rivelò progressivamente fallace, anche a causa della variabilità delle misurazioni e della possibilità di manipolazione, venendo infine soppiantato, all'inizio del XX secolo, dal più affidabile sistema di identificazione tramite impronte digitali. Per un approfondimento sulla figura e sul metodo di Bertillon, si veda A. BERTILLON, *La photographie judiciaire*, Parigi, 1890; invece, in relazione all'analisi di questo sistema cfr. S. AMATO - S. CRISTOFARI - S. RACITI, *Biometria: i codici a barre del corpo*, Torino, 2013, *passim*.

necessità di garantire una tutela adeguata ai diritti fondamentali della persona ¹⁴.

La scelta di considerare i dati biometrici non solo come dati personali, ma anche come dati particolari, riflette una consapevolezza giuridica dei rischi connessi al loro trattamento e conferma la centralità del principio di autodeterminazione informativa ¹⁵. In questo scenario, il legislatore europeo ha adottato un approccio che non si limita a fotografare lo stato dell'arte delle tecnologie biometriche, ma predispone una cornice normativa capace di adattarsi alle innovazioni future ¹⁶. Resta tuttavia aperta la questione della concreta applicazione di tali principi, in un

¹⁴ Pur non occupandosi in modo diretto dei dati biometrici, un contributo di particolare rilievo nell'ambito della riflessione costituzionale sul ruolo degli algoritmi nei processi decisionali incidenti sulle libertà fondamentali è rappresentato da A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal - Rivista di BioDiritto*, 2019, 1, p. 63 ss. L'analisi svolta dall'Autore offre spunti di sicuro interesse anche in chiave analogica, ove si consideri che il trattamento automatizzato dei dati biometrici, specie nei contesti di sorveglianza o profilazione predittiva, può determinare effetti strutturalmente simili, incidendo sulla libertà personale e sull'identità in forme che sollecitano una tutela costituzionale rafforzata.

¹⁵ Il diritto alla protezione dei dati personali può essere letto, in chiave evolutiva, come espressione di un più ampio diritto all'autodeterminazione informativa, concetto che ha trovato progressiva elaborazione a partire dalla giurisprudenza costituzionale tedesca e che si è ormai radicato anche nell'ordinamento europeo. In tale prospettiva, il controllo sui dati non si esaurisce in una mera prerogativa formale, ma diviene strumento essenziale per l'autogoverno della propria identità digitale, attraverso la facoltà di decidere consapevolmente quando, come e in che misura le informazioni personali possano essere comunicate, elaborate o condivise da terzi. Ciò implica un rapporto diretto tra la persona e l'informazione che la riguarda, in cui il dato personale non è un'entità neutra, bensì un'estensione dinamica della soggettività, capace di riflettere e determinare le traiettorie identitarie dell'individuo nell'ambiente digitale. L'autodeterminazione, dunque, non si limita alla scelta iniziale sul trattamento, ma include anche la possibilità di revoca, di opposizione, di modifica e di intervento attivo sul ciclo di vita informativo, secondo una logica di partecipazione effettiva e con-

tinua. In questo senso, il diritto alla protezione dei dati non riguarda esclusivamente la sicurezza dei flussi informativi, bensì la titolarità sostanziale della propria immagine informativa e la capacità della persona di conservare la sovranità su di essa. Si configura, pertanto, come un diritto fondante dell'individuo contemporaneo, intimamente connesso alla dignità, alla libertà personale e al libero sviluppo della personalità, in coerenza, come ampiamente noto, con quanto sancito dagli articoli 1, 2 e 8 della Carta dei diritti fondamentali dell'Unione europea e dagli articoli 1 e 2 della Costituzione italiana. Evidenzia il passaggio dalla tradizionale concezione della *privacy* come "diritto ad essere lasciati soli" al più moderno diritto al controllo sulle proprie informazioni personali, sottolineando l'importanza dell'autodeterminazione informativa, S. RODOTÀ, che esplora le implicazioni giuridiche di questa evoluzione, soffermandosi sulla necessità di tutelare l'identità personale nell'era digitale e proponendo una sistematizzazione dei principi fondamentali per la protezione dei dati personali. Cfr., S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, pp. 583.; nonché sul concetto di identità personale G. ALPA, *Diritti della personalità emergenti: profili costituzionali e tutela giurisdizionale. Il diritto alla identità personale*, in *Giur. merito*, 1989, pp. 464 ss. Di contro, sul principio di autodeterminazione informativa, in chiave comparatistica si veda G. BINCOLETTI, *Il diritto alla protezione dei dati: una prospettiva comparata*, in P. Guarda - G. Bincoletti (a cura di), *Diritto comparato della privacy e della protezione dei dati personali*, Milano, 2023, pp. 101 ss.

¹⁶ Nel tentativo di disciplinare in modo organico l'uso dei sistemi di intelligenza artificiale, e in particolare quelli fondati sull'elaborazione di dati biometrici, il legislatore europeo ha introdotto una cornice normativa avanzata e adattiva, destinata a reg-

contesto in cui la biometria è sempre più presente nella vita quotidiana e in cui i confini tra sicurezza e sorveglianza diventano sempre più labili.

2. DATI BIOMETRICI E PROFILAZIONE: IL CONFINE SOTTILE TRA IDENTITÀ E SORVEGLIANZA NELL'ERA DELL'INTELLIGENZA ARTIFICIALE.

Nel cuore dell'evoluzione digitale che segna il nostro tempo, i dati biometrici si configurano come il punto di convergenza tra corporeità e informazione, tra individualità e algoritmo. Essi rappresentano il tentativo di tradurre l'unicità fisica della persona — ciò che la distingue in modo irripetibile — in linguaggio computazionale, in codice. E non è un caso che, nella stagione normativa contemporanea, siano al centro di una rinnovata attenzione giuridica, segnatamente nel contesto dell'*Artificial Intelligence Act* (Regolamento UE 2024/1689), approvato per plasmare un ambiente normativo che sia insieme promotore dell'innovazione e presidio dei diritti fondamentali.

L'*AI Act*¹⁷, si presenta come un articolato tentativo di instaurare un ecosistema di fiducia per l'intelligenza artificiale, istituendo regole comuni che disciplinino l'uso della tecnologia se-

gere l'urto dell'innovazione tecnologica. Con il Regolamento (UE) 2024/1689 sull'intelligenza artificiale — di cui si dirà — si è inteso fornire una definizione giuridicamente puntuale delle nozioni centrali, capaci di orientare i trattamenti futuri. In particolare, l'art. 3, n. 34 del Regolamento qualifica, come già analizzato precedentemente, i *dati biometrici* come « *dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici* », ricalcando sostanzialmente l'art. 4, n. 14 del GDPR. Il successivo n. 35 introduce, invece, la nozione di identificazione biometrica, definita come « *il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati* ». Questa doppia definizione consente di articolare il perimetro applicativo della normativa e di calibrare le tutele in base alla rischiosità dei trattamenti, contribuendo così a delineare una cornice giuridica tecnologicamente neutra ma concretamente efficace, che si propone di regolare non soltanto lo stato dell'arte, ma anche i futuri sviluppi della biometria computazionale.

¹⁷ Il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, noto come "*AI Act*", è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea in data 12 luglio 2024 ed è entrato in vigore il 1° agosto dello stesso anno. Esso rappresenta il primo strumento giuridico sovranazionale volto a disciplinare organicamente l'intero ciclo di vita dei sistemi di intelligenza artificiale, dalla progettazione alla messa in commercio, fino all'utilizzo, secondo un approccio fondato sulla graduazione del rischio. Il Regolamento si propone di garantire un equilibrio tra l'esigenza di promuovere l'innovazione tecnologica e la necessità di proteggere i diritti fondamentali delle persone, con particolare attenzione alle implicazioni derivanti dal trattamento automatizzato di dati personali, tra cui quelli biometrici assumono un rilievo particolarmente critico. In parallelo, anche il legislatore italiano ha avviato un percorso normativo volto a integrare e accompagnare l'attuazione del quadro europeo, mediante l'approvazione, da parte del Consiglio dei Ministri, di un disegno di legge in materia di intelligenza artificiale, deliberato il 23 aprile 2024. Tale iniziativa, già oggetto di osservazioni da parte della Commissione europea, è stata approvata in prima lettura dal Senato il 20 marzo 2025 ed è attualmente all'esame della Camera dei Deputati. Tale percorso normativo

condo principi di affidabilità, trasparenza e sicurezza ¹⁸. Tra le numerose definizioni che il Regolamento fornisce, particolare rilievo assume quella contenuta all'art. 3, n. 34, relativa ai dati biometrici, intesi come « *dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici* ».

Questa definizione, che ricalca sostanzialmente quella già delineata dal Regolamento generale sulla protezione dei dati, non si limita a una classificazione lessicale: essa introduce una qualificazione giuridicamente decisiva, in quanto riconduce i dati biometrici alla categoria più ampia dei dati personali, connotandoli come “speciali” per via del trattamento tecnico che li genera. In altre parole, ciò che conferisce a un dato la natura “biometrica” non è la caratteristica corporea in sé — l'impronta digitale, la forma del volto, la voce — ma l'intervento tecnologico che la rileva, la isola e la struttura secondo modalità che ne permettano l'elaborazione automatizzata a fini identificativi.

Questa puntualizzazione non è affatto marginale. Al contrario, essa è il fulcro attorno a cui ruota l'intera problematica giuridica della profilazione biometrica, perché determina il momento in cui un'informazione, apparentemente neutra o generica, entra nello spazio protetto del dato sensibile e attiva le garanzie più elevate previste dall'ordinamento. È qui che si gioca la partita tra libertà individuale e potere tecnologico, tra il diritto alla propria immagine (e alla sua integrità) e le capacità invasive degli strumenti algoritmici.

evidenzia la volontà del legislatore nazionale di intervenire in settori chiave — tra cui sanità, pubblica amministrazione e mercato del lavoro — pur nella consapevolezza della necessità di una piena coerenza sistemica con l'*AI Act*, al fine di evitare disallineamenti interpretativi e garantire l'effettività del nuovo ecosistema giuridico europeo dell'IA.

¹⁸ In forma antesignana, sulla proposta di Regolamento sull'IA, si veda G. FINOCCHIARO, *La proposta di Regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in questa *Rivista*, 2022, 2, pp. 303 ss., ove l'Autrice approfondisce con chiarezza sistematica l'architettura normativa della proposta di *AI Act*, ponendo l'accento sul carattere preventivo del modello europeo, costruito secondo una logica di graduazione normativa fondata sulla valutazione del rischio. In tale prospettiva, l'intelligenza artificiale non viene regolata in astratto, ma attraverso

una tassonomia funzionale alle possibili ricadute su diritti fondamentali, sicurezza pubblica e interessi collettivi. Particolare attenzione è riservata ai sistemi di identificazione biometrica remota, espressamente collocati nella fascia di alto rischio, in quanto suscettibili di impattare in modo significativo sulla sfera privata e sull'identità personale degli individui. La riflessione si concentra, in particolare, sull'impianto degli obblighi preventivi previsti dal Regolamento — tra cui l'esecuzione obbligatoria di valutazioni d'impatto, l'adozione di misure tecniche e organizzative rafforzate, nonché l'obbligo di intervento umano significativo — al fine di assicurare il rispetto dei principi di trasparenza, non discriminazione e *accountability*. Il contributo rappresenta un riferimento imprescindibile per comprendere come il legislatore europeo stia cercando di coniugare innovazione tecnologica e tutela dei diritti fondamentali nel trattamento di dati ad alta densità sensibile, quali quelli biometrici.

Un esempio paradigmatico di tale tensione è rappresentato dal caso *Clearview AI*¹⁹, divenuto emblematico per la comprensione dei confini della nozione di dato biometrico. La società americana è nota per aver sviluppato un *software* di riconoscimento facciale fondato su un vasto *database* di immagini raccolte indiscriminatamente dalla rete, tramite tecniche di *web scraping*²⁰. Le fotografie — pubblicamente accessibili ma riferibili a soggetti identificabili — venivano elaborate attraverso modelli di *machine learning* che ne estraevano rappresentazioni vettoriali, funzionali a

¹⁹ Il caso *Clearview AI* rappresenta uno dei più rilevanti snodi interpretativi e normativi nel dibattito contemporaneo sul riconoscimento facciale. L'azienda statunitense, fondata nel 2017, ha realizzato un algoritmo in grado di identificare volti umani attraverso un *database* creato mediante *scraping* massivo di immagini da fonti pubblicamente accessibili *online*, incluse piattaforme sociali e siti *web* informativi. Questa prassi ha immediatamente sollevato critiche in relazione alla violazione della riservatezza e all'assenza di basi giuridiche per l'acquisizione e il trattamento di dati biometrici. Negli Stati Uniti, l'attività dell'azienda è stata oggetto di un'azione legale da parte dell'*American Civil Liberties Union* (ACLU), la quale ha contestato la violazione del *Biometric Information Privacy Act* dell'Illinois, che richiede il consenso esplicito per la raccolta di dati biometrici. L'accordo transattivo, raggiunto nel 2022, ha imposto a *Clearview AI* restrizioni sull'uso del proprio *database*, limitandone l'accesso ad autorità pubbliche e vietandone la vendita a soggetti privati. Un ulteriore sviluppo si è avuto nel marzo 2025, con l'approvazione da parte del tribunale federale di Chicago di un accordo collettivo che riconosce ai ricorrenti il diritto a una quota azionaria potenziale del 23% della società, subordinata a eventi futuri come la vendita o la quotazione in borsa. Anche a livello internazionale, la società è stata destinataria di plurime sanzioni. L'*Information Commissioner's Office* (ICO) britannico ha imposto, nel 2022, una multa di oltre 7 milioni di sterline e ha ordinato la cessazione del trattamento dei dati relativi a cittadini del Regno Unito. In Francia, la *Commission nationale de l'informatique et des libertés* (CNIL) ha comminato una sanzione di 20 milioni di euro per violazioni multiple del GDPR, con particolare riferimento all'assenza di base giuridica e al mancato rispetto dei diritti degli interessati. A ciò si è aggiunta, nel settembre 2024, una sanzione di 30,5 milioni di euro irrogata dall'autorità olandese, per la raccolta illegittima di dati biometrici senza il consenso degli interes-

sati. Nel febbraio 2025, infine, l'azienda ha annunciato un cambio ai vertici, con le dimissioni del fondatore Hoan Ton-That e la nomina alla guida della società di Hal Lambert e Richard Schwartz, in un momento segnato da pressioni regolatorie crescenti e da una rilevante esposizione reputazionale. Il caso *Clearview AI* si impone come snodo paradigmatico nel rapporto tra innovazione tecnologica, sorveglianza biometrica e tutela dei diritti fondamentali, imponendo una riflessione profonda sul bilanciamento tra esigenze di sicurezza e protezione dell'identità personale. Interessanti spunti di riflessione sul tema sono forniti, *ex multis*, da C. DUL, *Facial Recognition Technology vs Privacy: The Case of Clearview AI*, in *Queen Mary Law Journal*, 2022, Vol. 3, pp. 1-24; J. PIEMONTE - V. PAPAKONSTANTINO, *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 *Cib. e dir.*, 2023, Vol. 24, 73 (1), pp. 43-58.

²⁰ La pratica del *web scraping* — talvolta indicata anche con le espressioni *web harvesting* o *web data extraction* — rappresenta una modalità tecnologica funzionale all'estrazione automatizzata di contenuti disponibili *online*, effettuata attraverso *software* dedicati. Tali strumenti sono impiegati, in misura crescente, per alimentare i *dataset* su cui si basano i processi di addestramento degli algoritmi di intelligenza artificiale. In ragione della sua crescente diffusione e delle delicate implicazioni che comporta, tanto sul versante giuridico quanto su quello epistemologico e tecnico, la tecnica in parola è divenuta oggetto di un serrato dibattito dottrinale, che ne indaga i risvolti regolatori, i limiti di liceità e l'impatto sulle architetture informative contemporanee. Riflessioni sull'attività di *web scraping* sono riconducibili, tra gli altri, a B. TASSONE - M. BARBONE, *Web harvesting, scraping or data extraction, tutela delle banche dati secondo la legge sul diritto d'autore e i principi di diritto antitrust*, in *Diritto di Internet*, 2020, 1, pp. 113

una successiva attività di *matching* volto a individuare i soggetti raffigurati.

Ora, ciò che qui rileva non è soltanto la dimensione massiva e non consensuale della raccolta, quanto piuttosto la natura stessa del trattamento effettuato: le immagini statiche di individui, di per sé, non possono essere qualificate come dati biometrici secondo la definizione normativa vigente. Solo con l'applicazione di un processo tecnico specifico, volto a trasformare il dato visivo in una rappresentazione computazionale utilizzabile per finalità identificative, si verifica quel salto qualitativo che giustifica l'inquadramento giuridico del dato come "biometrico".

La distinzione, per quanto sottile, è fondamentale. Essa segna il *discrimen* tra un trattamento soggetto a regole generali sulla protezione dei dati personali²¹ e uno che ricade nell'ambito più restrittivo delle misure previste per i dati sensibili, con tutte le implicazioni in termini di liceità, proporzionalità e necessità. Ed è proprio questo passaggio — dall'immagine grezza al modello vettoriale — a rendere l'attività di *Clearview AI* illecita secondo diverse autorità garanti europee, poiché il trattamento effettuato presupponeva non solo un consenso informato, ma anche una base giuridica solida, che nel caso di specie era del tutto assente.

Alla luce di quanto detto, la relazione tra dati biometrici e profilazione si configura come uno dei terreni più delicati del diritto contemporaneo. La profilazione, intesa come ogni forma di trattamento automatizzato finalizzato a valutare aspetti personali di un individuo, trova nei dati biometrici un materiale privilegiato

ss; P. SAMMARCO, *L'attività di web scraping nelle banche dati e il riuso delle informazioni*, in questa Rivista, 2020, 219; A. QUARTA - M. W. MONTEROSSO, *Web Scraping: A Private Law Perspective*, in *i-lex - Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, 2023, Vol. 16, 2, pp. 46 ss.; J. TORRE DE SILVA - L. DE LETONA, *The Right to Scrape Data on the Internet: From the US Case hiQLabs, Inc. v. LinkedIn Corp. to the ChatGPT Scraping Cases: Differences Between US and EU Law*, in *Global Privacy Law Review*, 2024, Vol. 5, 1, pp. 5 ss.

²¹ Ai fini di una panoramica sullo sviluppo concettuale della *data protection*, si rimanda, in via orientativa, a S. RODOTÀ, *La privacy tra individuo e collettività*, in *Pol. dir.*, 1974, pp. 550 ss.; V. CUFFARO, V. RICCIUTO, (a cura di), *La disciplina di dati personali*, Torino, 1997; S. SICA, *Danno morale e legge sulla privacy informatica*, in *Danno e resp.*, 1997, pp. 282 ss.; G. ALPA, *Aspetti della disciplina sui dati personali riguardanti gli enti e l'attività economica. Profili civilistici*, in *Econom. dir. terziario*,

1998, pp. 331 ss.; Id., *La disciplina dei dati personali. Note esegetiche sulla l. 31.12.1996, n. 675 e successive modifiche*, Roma, 1998; S. SICA, *Decreto legislativo n. 171/98: Commento*, in *Corriere giur.*, 1998, p. 1004; C.M. BIANCA - F.D. BUSNELLI (a cura di), *La tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, pp. 219 ss.; D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1999, p. 339; G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2000, pp. 299; S. SICA, *Danno morale per lesione della privacy: domicilio ed essenzialità della notizia*, in questa Rivista, 2000, p. 469; Id., *Commento agli artt. 18 e 29, comma 9, l. 675/96*, in E. GIANNANTONIO - M. LOSANO - V. ZENO-ZENCOVICH, *La tutela dei dati personali*, Padova, 2001; Id., *D.lgs. n. 467/01 e "riforma" della privacy: un vulnus al « sistema » della riservatezza*, in questa Rivista, 2002, pp. 263 ss.; S. SICA - V. D'ANTONIO - G.M. RICCIO, *La nuova disciplina europea della Privacy*, Milanofiori Assago (MI), 2016.

per la costruzione di identità digitali e, di riflesso, per l'esercizio di poteri selettivi, discriminatori, persino predittivi.

Ecco allora che il problema non è solo tecnico, né soltanto giuridico: è antropologico. Come ricordava Stefano Rodotà, la protezione dei dati personali non è altro che la protezione della persona nella sua interezza, nella sua dignità²². Il dato biometrico, proprio perché attiene alla dimensione corporea più profonda e irripetibile dell'individuo, deve essere trattato con la massima cautela, come se si trattasse di una porzione della persona stessa. E ogni intervento normativo, come ogni innovazione tecnologica, è chiamato a misurarsi con questa esigenza di tutela, che non è solo giuridica, ma etica, civile, democratica.

Apertis verbis, la qualificazione e il trattamento dei dati biometrici non possono essere considerati una questione meramente definitoria. Essi rappresentano, invece, una cartina di tornasole della capacità del diritto di fronteggiare le nuove forme di potere algoritmico, ponendo limiti chiari e riconoscibili al loro esercizio. Solo in questo modo l'intelligenza artificiale potrà davvero inserirsi in un quadro che sia, al contempo, tecnologicamente evoluto e pienamente rispettoso dei diritti fondamentali della persona.

Nel percorso di affinamento concettuale del dato biometrico, un passaggio ulteriore e decisivo è rappresentato dal confronto tra le definizioni offerte dal GDPR e quelle contenute nell'*AI Act*. In particolare, si rende evidente la presenza di un ulteriore criterio strutturale, implicito ma fondamentale: la possibilità di identificare in modo univoco una persona fisica a partire dal dato oggetto di trattamento.

Questo profilo è stato recentemente riaffermato con chiarezza dalla Corte di Cassazione, nella sentenza n. 12967 del 13 maggio 2024²³. In tale occasione, la Suprema Corte ha confermato la sanzione irrogata dal Garante per la protezione dei dati personali nei confronti di un istituto universitario, affermando un principio

²² In particolare, ci si riferisce a S. Rodotà che ha trattato queste tematiche in vari scritti, tra cui il discorso conclusivo alla 26^a Conferenza internazionale sulla protezione dei dati, intitolato: "*Privacy, libertà, dignità*". *Discorso conclusivo della Conferenza internazionale sulla protezione dei dati. Trattasi del Conclusive Remarks at the 26th International Conference on Privacy and Personal Data Protection*, tenutasi in Polonia, a Wroclaw, dal 14 al 16 settembre 2004.

²³ La Corte ha affrontato il caso di un'università italiana che, durante l'emergenza pandemica, aveva adottato un *software* per monitorare lo svolgimento degli esami a distanza. Questo sistema catturava immagini e video degli studenti, segnalando

eventuali comportamenti anomali mediante registrazioni e fotografie scattate a intervalli casuali. Il Tribunale di Milano, in primo grado, aveva ritenuto che tale attività non configurasse un trattamento di dati biometrici, considerando che l'identificazione degli studenti avveniva successivamente ad opera dei docenti. La Corte di Cassazione ha ribaltato questa decisione, stabilendo che l'utilizzo del *software* in questione integrava un trattamento di dati biometrici ai sensi dell'art. 9 del GDPR. Ha sottolineato che, anche se l'esito del trattamento automatizzato è successivamente valutato da un operatore umano, ciò non modifica la natura del trattamento stesso. Sul punto, si veda *Trattamento illecito di dati biometrici* (Ord. Cass. Civ. Sez. I, n. 12967, 2024) in

di diritto di notevole rilievo sistemico: si configura un trattamento di dati biometrici, ai sensi dell'art. 9 GDPR, quando il dato personale è ottenuto mediante un procedimento tecnico automatizzato — quale un *software* che analizza caratteristiche fisiche, fisiologiche o comportamentali — e che produce un risultato (ad esempio un'immagine o un'elaborazione video) idoneo a consentire l'identificazione univoca della persona. La successiva verifica da parte di un operatore umano non incide sulla natura del trattamento, che resta qualificabile come biometrico.

L'interesse di tale pronuncia non si esaurisce nella sua portata applicativa, ma assume valore strutturale, poiché ribadisce che il nesso tra dato biologico e identificazione personale rappresenta il cuore della disciplina. Un'affermazione che, pur nella formulazione differente, trova eco anche nell'*AI Act*, dove l'art. 3, n. 35, definisce l'« identificazione biometrica » come il processo automatizzato volto a determinare l'identità di una persona fisica mediante confronto dei suoi dati biometrici con quelli contenuti in una banca dati ²⁴.

A ben vedere, questa introduzione terminologica non innova sostanzialmente, ma esplicita una componente già immanente nella nozione stessa di dato biometrico così come delineata all'art. 4, n. 14 del GDPR. L'identificazione, dunque, non è una funzione eventuale, ma un tratto distintivo del trattamento biometrico, che rende necessario un regime rafforzato di tutela.

La dottrina prevalente ²⁵ ha già da tempo sottolineato questo legame indissolubile, riconoscendo che il dato biometrico non si esaurisce nella sua dimensione materiale o nel mero trattamento tecnico, ma si compie nel momento in cui viene impiegato per ricostruire — con finalità identificative — il profilo della persona fisica. Tale posizione è stata altresì fatta propria dal Comitato europeo per la protezione dei dati (EDPB), il quale, nelle Linee guida 3/2019 sul trattamento dei dati personali mediante dispositivi video, ha evidenziato tre elementi qualificanti del dato biometrico: la natura dei dati (legata a caratteristiche fisiche, fisio-

Diritto di Internet, approfondimento a cura della Redazione nella sezione "News e Giurisprudenza" della Rivista.

²⁴ Testualmente: « *Biometric categorisation' means the automated assignment of natural persons to specific categories on the basis of their biometric data, including characteristics, features or traits relating to physical, physiological, behavioural or psychological characteristics* ».

²⁵ Che pur non usando espressamente questa formula, ha posto il trattamento biometrico all'intersezione fra corpo, dignità e identità, chiarendo che la protezione non può essere circoscritta all'elemento tecnico

il riferimento, tra gli altri, è a S. RODOTÀ, *Il mondo nella rete: quali i diritti, quali i vincoli*, Bari-Roma, 2014, *passim*. L'Autore analizza con acutezza le profonde implicazioni che derivano dalla sistematica raccolta e conservazione, da parte di attori pubblici e privati, delle informazioni personali fornite spontaneamente dagli individui nell'ambiente digitale, evidenziando come tale fenomeno possa compromettere le tradizionali garanzie del diritto liberale, ponendo in discussione l'effettivo controllo dell'individuo sui propri dati e la stessa configurazione dell'identità personale nella dimensione *online*.

logiche o comportamentali), il trattamento tecnico specifico e, in modo cruciale, la finalità di identificazione univoca²⁶.

Non sorprende, dunque, che le Autorità di protezione dati abbiano assunto un approccio particolarmente prudente in materia. In Italia, il Garante Privacy, nel Provvedimento n. 146 del 5 giugno 2019, ha imposto specifiche misure di garanzia nel trattamento delle categorie particolari di dati, imponendo l'adozione di tecniche idonee a minimizzare il rischio identificativo, specie nei trattamenti automatizzati. Ancora più recentemente, con provvedimento del 22 febbraio 2024, il Garante ha vietato l'archiviazione remota dei dati biometrici raccolti per finalità di autenticazione, ribadendo che la conservazione debba avvenire esclusivamente sul dispositivo dell'interessato, a tutela del principio di minimizzazione e di sicurezza²⁷.

A completamento della prospettiva ricostruttiva sinora sviluppata, giova proporre un affresco comparatistico che restituisca la

²⁶ Nel contesto della disciplina sulla protezione dei dati personali, un contributo ermeneutico di particolare rilievo è fornito dalle Linee guida 3/2019 del Comitato europeo per la protezione dei dati (EDPB), dedicate al trattamento dei dati personali attraverso dispositivi video. In tale documento, l'EDPB chiarisce con metodo che non ogni immagine o ripresa visiva rientra automaticamente nella nozione di "dato biometrico" ai sensi dell'art. 4, punto 14, del GDPR. Perché si possa configurare un dato come tale, è necessario che concorrano specifici requisiti, articolati su un triplice piano: innanzitutto, la natura dei dati deve riferirsi a caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, idonee a distinguere in maniera individuale; in secondo luogo, tali caratteristiche devono essere sottoposte a un trattamento tecnico specifico, vale a dire una trasformazione operata da procedure automatizzate che estraggano informazioni biometricamente rilevanti; infine, è cruciale che la finalità perseguita attraverso il trattamento sia l'identificazione univoca o l'autenticazione della persona. È dunque il combinato disposto di questi tre elementi — natura fisica o comportamentale, trattamento tecnico dedicato, e finalità identificativa — a determinare il salto qualitativo tra semplice immagine e dato biometricamente rilevante. In assenza anche di uno solo di tali presupposti, non si realizza la soglia normativa che attiva l'applicazione delle cautele rafforzate previste dal Regolamento, in particolare quelle di cui all'art. 9 GDPR. Ne deriva una responsabilità interpretativa particolarmente stringente in capo ai titolari del trattamento, i quali devono compiere una valu-

tazione *ex ante* che tenga conto non solo del contenuto intrinseco dei dati, ma anche delle modalità e degli scopi concreti della loro elaborazione. Questo approccio sistemico, d'impronta sostanzialista, riflette la necessità di coniugare tutela della persona, controllo algoritmico e garanzie procedurali all'interno di un quadro giuridico che riconosce ai dati biometrici un potenziale fortemente intrusivo sulla sfera identitaria del soggetto. Per un'analisi critica delle pratiche di sorveglianza visiva e biometrica nell'Unione Europea, facendo riferimento alle Linee guida 3/2019 dell'EDPB e discutendo delle implicazioni per la protezione dei dati personali, si veda quanto sostenuto da P. DE HERT - G. BOUCHAGIAR, *Visual and biometric surveillance in the EU. Saying 'no' to mass surveillance practices?*, in *Information Policy*, 2022, Vol. 27, 1, pp. 193 ss.

²⁷ Il Garante per la protezione dei dati personali italiano, con il Provvedimento n. 146 del 5 giugno 2019, ha delineato specifiche prescrizioni riguardanti il trattamento di categorie particolari di dati personali nell'ambito dei rapporti di lavoro. Tale provvedimento, pubblicato nella Gazzetta Ufficiale n. 176 del 29 luglio 2019, si applica a tutti i soggetti che, a vario titolo, effettuano trattamenti per finalità connesse all'instaurazione, gestione ed estinzione del rapporto di lavoro. In particolare, il Garante ha enfatizzato l'importanza di adottare misure tecniche e organizzative adeguate per garantire la sicurezza dei dati e minimizzare i rischi per i diritti e le libertà degli interessati, soprattutto nei trattamenti automatizzati. Ciò include l'impiego di tecniche idonee a ridurre il rischio identificativo, in conformità ai principi di minimizzazione e

sostanziale convergenza degli orientamenti giuridici maturati nei principali ordinamenti, i quali — pur nella varietà dei contesti — esprimono una linea coerente di tutela rispetto ai profili più sensibili del trattamento biometrico. In Francia, la CNIL ha vietato l'uso del riconoscimento facciale nelle scuole di Nizza, ritenendo sproporzionato il trattamento rispetto alla finalità perseguita, e dunque non compatibile con i principi del GDPR. In Germania, l'Autorità del *Baden-Württemberg* ha assunto una linea analoga, vietando l'uso del riconoscimento facciale per l'accesso scolastico, ritenendo il trattamento lesivo della dignità e della libertà dei minori ²⁸.

Alla luce di queste prassi consolidate, l'apparente perdita di centralità del concetto di identificazione nella definizione dell'*AI Act* deve essere interpretata non come un'attenuazione del requisito, ma come una sua rinnovata autonomia sistematica. Si delinea così un quadro normativo in cui l'identificazione assume un ruolo

proporzionalità previsti dal Regolamento (UE) 2016/679 (GDPR). Successivamente, con il Provvedimento del 22 febbraio 2024, il Garante ha affrontato la questione dell'archiviazione dei dati biometrici utilizzati per finalità di autenticazione nell'ambito lavorativo. In tale contesto, l'Autorità ha ribadito che i dati biometrici degli interessati devono risiedere esclusivamente nel dispositivo dell'interessato e non essere accessibili da remoto né in locale, se non per la cancellazione, che può essere effettuata solo direttamente sul dispositivo. Questa disposizione sottolinea l'importanza di evitare l'archiviazione remota dei dati biometrici, al fine di tutelare il principio di minimizzazione e garantire un elevato livello di sicurezza nel trattamento di informazioni particolarmente sensibili. I Provvedimenti emanati dall'Autorità italiana sono consultabili ai seguenti link di riferimento: « <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9124510> »; « <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995680> ».

²⁸ Nel contesto europeo, il trattamento dei dati biometrici in ambito scolastico è stato oggetto di un severo scrutinio da parte delle autorità garanti, in ragione della vulnerabilità dei minori e della sproporzione tra le finalità dichiarate e i mezzi tecnologici impiegati. Di particolare rilievo è l'intervento della *Commission nationale de l'informatique et des libertés* (CNIL), che ha censurato il progetto sperimentale avviato in due licei della regione Provenza-Alpi-Costa Azzurra (Nizza e Marsiglia), volto all'introduzione del riconoscimento facciale per il controllo degli accessi scolastici. L'Autorità ha ritenuto che tale pratica, lungi

dall'essere necessaria, violasse i principi di liceità, minimizzazione e proporzionalità di cui agli artt. 5, par. 1, lett. c), e 9 del GDPR, anche in considerazione dell'assenza di alternative meno invasive e della delicatezza del contesto formativo. A ciò si aggiunge la preoccupazione di fondo circa l'introduzione, in ambienti educativi, di tecnologie che rischiano di normalizzare forme di sorveglianza pervasiva, compromettendo lo sviluppo libero della personalità dei minori. Un orientamento speculare è stato assunto in Germania, dove l'Autorità del *Baden-Württemberg* ha vietato l'impiego del riconoscimento facciale per il rilevamento delle presenze scolastiche, rilevando l'incompatibilità del trattamento con i principi del GDPR e sottolineando la lesione del diritto alla dignità e alla libertà degli studenti. Anche in questo caso, l'assenza di una base giuridica adeguata e la disponibilità di mezzi alternativi meno invasivi hanno indotto l'Autorità a concludere per l'illiceità del trattamento. Entrambi i provvedimenti mostrano come l'impiego di tecnologie biometriche in ambienti educativi debba essere oggetto di una valutazione rigorosa *ex ante*, che tenga conto non solo dell'efficacia tecnica della misura, ma anche dell'impatto sistemico sull'identità digitale e sulla sfera esistenziale del soggetto vulnerabile. La protezione dei dati biometrici dei minori, in quanto proiezione corporea e identitaria della persona, impone un'attenzione rafforzata che travalica le esigenze di gestione organizzativa, riaffermando il primato della persona sulle logiche dell'efficienza tecnologica. Per approfondire analiticamente la questione si vedano il Comunicato ufficiale del CNIL, *Communiqué de presse du 30 octobre*

trasversale, fungendo da criterio interpretativo per valutare la liceità e proporzionalità del trattamento stesso.

In definitiva, il dato biometrico non può essere considerato un mero sottoprodotto tecnico della corporeità digitalizzata, ma deve essere inteso come dispositivo giuridico complesso, che, nella sua capacità di consentire il riconoscimento individuale, solleva interrogativi profondi in materia di libertà, sorveglianza e dignità personale. È proprio in questa prospettiva che il diritto è chiamato non solo a disciplinare l'uso dei dati biometrici, ma a governarne le implicazioni sistemiche, garantendo che l'innovazione non diventi veicolo di controllo pervasivo, bensì strumento di progresso conforme ai diritti fondamentali dell'individuo.

3. DAI TRATTI DEL VOLTO AI TRATTI DELL'IDENTITÀ: IL PASSAGGIO DALLA BIOMETRIA ALLA PROFILAZIONE.

Una volta chiarito che il dato biometrico rappresenta un elemento identitario ad alta densità informativa, risulta pressoché inevitabile estendere la riflessione alla questione della profilazione, come forma ulteriore e spesso non dichiarata del trattamento. Se l'identificazione univoca è il primo livello di impiego dei dati biometrici, la costruzione di profili comportamentali, predittivi o valutativi rappresenta la naturale — e per certi versi pericolosa — evoluzione di queste tecnologie.

L'art. 4, n. 4 del GDPR definisce la profilazione come « *qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica* ». La norma non menziona espressamente i dati biometrici, ma è evidente che questi, per la loro natura e il loro potenziale, possono rappresentare il substrato informativo più sensibile e penetrante per finalità di profilazione.

L'impiego di dati biometrici — specie nel contesto di strumenti dotati di intelligenza artificiale — non si esaurisce nella mera identificazione del soggetto, ma tende progressivamente a costruire modelli comportamentali in grado di anticipare scelte, emozioni, persino tratti psicologici dell'individuo. In questo senso,

2019, *La reconnaissance faciale au lycée: la CNIL précise les conditions de mise en œuvre dans les établissements scolaires* al link di riferimento: « <https://www.cnil.fr/fr/la-reconnaissance-faciale-au-lycee-la-cnil-precise-les-conditions-de-mise-en-oeuvre> » e quello del LfDI Baden-Württemberg, *Stellungnahme zur Gesichtserkennung an Schulen*, 2020, ove ampia sintesi in inglese è disponibile su: « [https://www.baden-](https://www.baden-wuerttemberg.datenschutz.de/en)

[wuerttemberg.datenschutz.de/en](https://www.baden-wuerttemberg.datenschutz.de/en) ». Anche autorevole dottrina si è espressa in tema di riconoscimento facciale, cfr. L. LEE-MORRISON, *Portraits of Automated Facial Recognition. On Machinic Ways of Seeing the Face*, Bielefeld, 2019, pp. 15 ss.; K.A. WONG, *The Face-ID Revolution: The Balance Between Pro-market and Pro-consumer Biometric Privacy Regulation*, in *J. High Tech. Law*, 2020, Vol. 20, 1, pp. 267 ss.

la biometria si fa semantica: dal riconoscimento del volto si passa al riconoscimento del carattere; dalla posizione del corpo, si inferiscono intenzioni; dal battito cardiaco, si tracciano stati emotivi ²⁹. L'informazione corporea si trasforma in informazione identitaria predittiva.

Tale passaggio, tutt'altro che neutro, solleva interrogativi profondi sul piano dei principi di necessità, proporzionalità e minimizzazione del trattamento, soprattutto quando la profilazione incide su ambiti decisionali automatizzati. Si pensi, ad esempio, all'uso dei dati biometrici nella sorveglianza predittiva, nei processi di selezione del personale, nella valutazione del rischio assicurativo o nei sistemi di *credit scoring*: in tutti questi contesti, la profilazione biometrica rischia di generare un algoritmo valutativo opaco, sfuggente, e perciò potenzialmente discriminatorio ³⁰.

È in questa prospettiva che l'*AI Act*, nel tentativo di anticipare i rischi legati all'uso dell'intelligenza artificiale, ha introdotto una classificazione dei sistemi biometrici tra gli usi ad alto rischio ³¹, sottoponendoli a un regime di vigilanza rafforzata. L'art. 6 e l'Allegato III del Regolamento contemplano espressamente i « sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico » tra le tecnologie suscettibili di pregiudicare diritti e libertà fondamentali ³². Ma accanto al tema della sorveglianza, si apre quello, forse più sottile, della manipolazione.

²⁹ Cfr., S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019. L'A. analizza come i dati comportamentali — tra cui postura, microespressioni, ritmo cardiaco — vengano sfruttati per prevedere e influenzare le condotte individuali, con particolare attenzione alle forme di “dispositional engineering”.

³⁰ Per un'analisi in chiave anche critica degli effetti che l'opacità algoritmica può produrre sul piano dell'eguaglianza sostanziale e dei diritti fondamentali si rinvia a M. BARBERA, *Discriminazioni algoritmiche e forme di discriminazione*, in *Labour & Law Issues*, 2021, Vol. 7, 1, pp. 3 ss.; S. TOMMASI, *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo*, in *Revista de Direito Brasileira*, 2021, Vol. 27, 10, pp. 112 ss.; E. FALLETTI, *Discriminazione algoritmica. Una prospettiva comparata*, Torino, 2022, *passim*; Id., *Algoritmi: la discriminazione non è uguale per tutti*, in *Lavoro Diritti Europa. Rivista nuova di Diritto del Lavoro*, 2023, 2, pp. 2 ss.

³¹ Si veda, A. MANTELEO - G. RESTA - G.M. RICCIO (a cura di), *Intelligenza artifi-*

ciale. Commentario. Regolamento (UE) 2024/1689 - AI ACT Linee guida Commissione europea pratiche vietate Disegno di legge sull'intelligenza artificiale, Milano, 2025, pp. 184 ss. Difatti, nella Sezione I, dedicata alla “Classificazione dei sistemi di IA come « ad alto rischio »”, gli Autori non si limitano a delineare i criteri generali che presiedono a tale qualificazione, ma specificano altresì che tra gli ambiti espressamente ricompresi rientrano anche i sistemi biometrici, i quali vengono così annoverati tra gli usi dell'intelligenza artificiale considerati particolarmente sensibili e ad elevato rischio.

³² Sulla qualificazione normativa dei sistemi di identificazione biometrica remota in tempo reale si veda l'art. 6(2) e l'Annex III, point 1(a) del Regolamento (UE) 2024/1689 (*AI Act*), ove si stabilisce quanto segue: “High-risk AI systems pursuant to paragraph 1 are the AI systems listed in Annex III”, tra cui rientrano:

“Remote biometric identification systems. This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she

Un volto non è solo un identificativo: può diventare un'interfaccia, un punto di accesso per inferenze automatizzate su abitudini, preferenze, emozioni. Così, l'identità rischia di diventare profilo, e il profilo, strumento di controllo.

La Corte di Giustizia dell'Unione Europea, nella nota sentenza *Schrems II* (C-311/18), pur non affrontando direttamente la questione biometrica, ha tuttavia ricordato che l'essenza del diritto alla protezione dei dati risiede nella capacità del soggetto di conoscere, controllare e limitare il trattamento dei propri dati personali³³. Questo principio trova la sua massima espressione proprio nella profilazione³⁴ automatizzata, dove la possibilità per l'individuo di reagire, comprendere e contestare il trattamento si fa sempre più esile.

claims to be." Il riferimento testuale è contenuto nel Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, pubblicato nella Gazzetta Ufficiale dell'Unione Europea L. 310 del 13 giugno 2024, pp. 1-95.

³³ La sentenza *Schrems II* della Corte di Giustizia dell'Unione Europea (C-311/18, 16 luglio 2020), come noto, rappresenta un vero spartiacque nel sistema europeo di protezione dei dati personali, poiché, pur non affrontando direttamente il tema dei dati biometrici, afferma con forza alcuni principi strutturali del diritto alla protezione dei dati, destinati a incidere trasversalmente su ogni tipologia di trattamento, anche automatizzato e ad alto impatto, come quello biometrico. Nel caso di specie, la Corte era chiamata a valutare la validità della decisione di adeguatezza denominata "*Privacy Shield*", che regolava i flussi di dati personali tra Unione Europea e Stati Uniti. La controversia prende origine dalle denunce di Maximilian Schrems, giurista e attivista austriaco, nei confronti di *Facebook Ireland Ltd.*, ritenuta responsabile del trasferimento dei dati degli utenti europei verso i server statunitensi della casa madre, in un contesto nel quale la normativa americana non garantiva, secondo il ricorrente, un livello di tutela equivalente a quello richiesto dal diritto europeo. Nella sua articolata motivazione, la Corte ha annullato la decisione della Commissione europea sullo "scudo per la *privacy*", ritenendola inadeguata alla luce dell'art. 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea e dell'art. 45 del GDPR. In particolare, la Corte ha ribadito che il diritto alla protezione dei dati non può ridursi a una mera garanzia formale o procedurale, ma deve esprimersi in un controllo concreto ed effettivo da parte dell'interessato sulla circolazione e l'uso delle proprie informazioni per-

sonali. La portata sistemica di *Schrems II* si coglie nella riaffermazione del principio secondo cui l'essenza del diritto alla protezione dei dati risiede nella capacità del soggetto di conoscere, controllare e circoscrivere il trattamento. Questo profilo, sebbene maturato in un contesto di trasferimento transfrontaliero, si proietta con forza anche nei trattamenti biometrici, ove l'asimmetria informativa e la complessità tecnica delle operazioni possono impedire all'interessato un'effettiva consapevolezza e autodeterminazione. In tal senso, la pronuncia della Corte costituisce un importante parametro ermeneutico per leggere il trattamento dei dati biometrici attraverso la lente della dignità e dell'autonomia del soggetto, riaffermando un modello di protezione sostanziale che non può essere sacrificato in nome dell'efficienza tecnologica o dell'interesse economico. Si segnalano gli estremi di riferimento, CGUE, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems*, causa C-311/18, sentenza del 16 luglio 2020. Il testo della pronuncia è disponibile in italiano su «eurlex.europa.eu». Numerosi sono gli Autori che hanno commentato la nota sentenza, tra i tanti, si veda, A. FLOR, *The Impact of Schrems II: Next Steps for U.S. Data Privacy Law*, in *Notre Dame Law Review*, 2021, Vol. 96, 5, pp. 2035 ss.

³⁴ Per ulteriori approfondimenti dottrinali in materia di profilazione, v. anche R. DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in questa *Rivista*, 2013, pp. 588; S. ACETO DI CAPRICIA, *Contrattazione algoritmica. Problemi di profilazione e prospettive operazionali. L'esperienza "pilota" statunitense*, in *Federalismi.it*, 2019, 18, pp. 2 ss.; G. SARTOR - F. LACIOIA, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi.it*, 2020, 11, pp. 85 ss.

In termini più ampi, siamo di fronte a un rovesciamento epistemologico: mentre il diritto tradizionalmente protegge ciò che l'individuo è, l'algoritmo pretende di tutelare ciò che l'individuo potrebbe essere, secondo modelli predittivi che sfuggono alla logica della trasparenza e della verificabilità. È qui che la profilazione incrocia il rischio dell'eterodeterminazione digitale dell'identità: non più il soggetto che si definisce attraverso la propria autodeterminazione, ma l'algoritmo che lo definisce attraverso correlazioni statistiche.

In questa prospettiva, il dato biometrico profilato si presenta come una forma nuova e sofisticata di potere informativo, che non si limita a rilevare, ma che interpreta, orienta, anticipa. Il diritto, allora, non può limitarsi a sorvegliare la liceità del trattamento, ma deve presidiare la sua finalità e impedire che il corpo diventi un campo di lettura automatica dell'identità, senza filtro, senza mediazione, senza consenso realmente informato.

Nel solco già tracciato dall'analisi della profilazione biometrica a fini pubblicitari, merita attenzione un ulteriore sviluppo della riflessione, che riguarda le forme più pervasive di tracciamento comportamentale *online*, attuate mediante tecnologie sofisticate di raccolta e analisi dei dati: è il caso emblematico dell'*Online Behavioural Advertising* (OBA)³⁵. In questo contesto, l'utilizzo diretto o indiretto di dati biometrici — anche dedotti da segnali corporei, posture, tracciamento oculare o micro-espressioni — alimenta sistemi di *targeting* altamente personalizzati, basati su un'osservazione continua e profondamente fisicizzata dell'interazione tra corpo e ambiente digitale³⁶.

Il cuore di tali pratiche è rappresentato dai *tracker* biometrici comportamentali, strumenti che operano in *background* sui dispositivi dell'utente e raccolgono non solo dati di navigazione, ma anche informazioni fisiologiche o psicofisiche, attraverso sensori integrati in *smartphone*, *webcam*, dispositivi indossabili. I dati raccolti — pur non sempre qualificati formalmente come biometrici — soddisfano i requisiti del GDPR e dell'*AI Act* quando derivano da trattamenti tecnici specifici idonei a identificare

³⁵ Per un'analisi approfondita dell'*Online Behavioural Advertising* e dei suoi potenziali effetti lesivi, anche in materia consumeristica, si veda J. LAUX - S. WACHTER - B. MITTELSTADT, *Neutralizing Online Behavioural Advertising Algorithmic Targeting with Market Power as an Unfair Commercial Practice*, in *Common Market Law Review*, 2021, Vol. 58, 3, pp. 719 ss.

³⁶ Sui sistemi di *targeting* e l'attività di pubblicità personalizzata online, si veda G. D'IPPOLITO, *Profilazione e Pubblicità Tar-*

gettizzata On-Line: Real-Time Bidding e Behavioural Advertising, Napoli, 2021, pp. 93 ss.; Ancora, sempre in tema di OBA e pubblicità personalizzata è di primario rilievo quanto sancito con la sentenza CGUE, 4 luglio 2023, C-252/21, *Meta c. Bundeskartellamt*, con nota di Id., *Data economy: la Corte di giustizia precisa il rapporto tra concorrenza e protezione dei dati personali e le norme sulla pubblicità personalizzata*, in *Media Laws - Rivista di Diritto dei Media*, 2023, 2, pp. 323 ss.

univocamente o a profilare la persona in base a caratteristiche del corpo o del comportamento.

Sul piano normativo, l'interazione tra GDPR, Direttiva *ePrivacy* e UCPD³⁷ si traduce in un quadro multilivello che impone limiti rigorosi all'uso di tali tecnologie, esigendo un consenso informato, libero e preventivo³⁸. Il consenso, come affermato dalla CGUE nella sentenza C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV* contro *Planet49 GmbH*, (c.d. "Planet 49"), non può mai essere presunto, né può derivare da impostazioni

³⁷ La Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, nota come *Unfair Commercial Practices Directive* (d'ora in avanti UCPD), rappresenta il quadro normativo di riferimento per la regolazione delle pratiche commerciali tra imprese e consumatori nell'Unione europea. Essa vieta, in particolare, ogni condotta commerciale che, per modalità o contenuti, sia idonea a distorcere in misura rilevante il comportamento economico del consumatore medio, con particolare riguardo alle pratiche ingannevoli (artt. 6-7) e aggressive (artt. 8-9). Recepita nell'ordinamento italiano attraverso il Codice del Consumo (d.lgs. n. 206/2005, artt. 18 ss.), la direttiva si fonda su un paradigma volto a garantire la libertà di autodeterminazione del consumatore attraverso la trasparenza e la lealtà informativa. Tale strumentazione giuridica assume un ruolo cruciale nel contesto dell'*Online Behavioural Advertising*. Questa pratica, pur dichiaratamente orientata al miglioramento dell'esperienza d'uso e della pertinenza degli annunci, espone l'utente a rischi significativi sotto il profilo della protezione dei dati e della libertà decisionale, configurando, nei casi più critici, forme di influenza indebita o sfruttamento di *bias* cognitivi. Alla luce della crescente pervasività delle tecnologie pubblicitarie (*adtech*), si è fatta strada una lettura della UCPD che ne valorizza la funzione anche in chiave di *consumer protection* digitale, riconoscendo che la vulnerabilità dell'utente *online* non si esaurisce nei profili *privacy*, ma investe più ampiamente la sua posizione di soggetto economico e di cittadino, esposto a dinamiche opache e spesso asimmetriche di persuasione automatizzata. La crescente complessità dell'ecosistema digitale, dominato da attori dotati di significativo potere di mercato, impone dunque un'interpretazione evolutiva della direttiva, in grado di affrontare le sfide poste dalle nuove forme di intermediazione algoritmica. Un riferimento all'interconnessione tra consumatori, *GBA* e *privacy* è offerto da J. CHEN, *Regulating On-*

line Behavioural Advertising Through Data Protection Law, Cheltenham, 2021, pp. 89-110.

³⁸ In relazione alla tematica del consenso giova richiamare un recente e significativo intervento (Prov. n. 114 del 27 febbraio 2025) con il quale il Garante per la protezione dei dati personali ha ribadito con fermezza l'inammissibilità dei cosiddetti "consensi *omnibus*" nell'ambito del trattamento dei dati personali per finalità di *marketing*. L'Autorità ha chiarito come la libertà del consenso non possa essere considerata effettiva quando l'interessato si trovi dinanzi a formule indistinte e cumulativo-omnicomprensive, che non gli consentano di operare una scelta consapevole e selettiva rispetto ai diversi utilizzi dei propri dati. La pretesa validità di un consenso reso in termini generici, senza possibilità di discernimento tra le differenti categorie merceologiche e i soggetti terzi destinatari del dato, compromette l'intero impianto di autodeterminazione informativa, fondato sul principio della specificità del consenso (art. 4, n. 11 e art. 7 GDPR). Il provvedimento in esame ha preso le mosse da un'indagine ispettiva nei confronti di una società operante nel settore della fornitura di energia elettrica e gas, sanzionata per avere acquisito consensi mediante moduli in cui l'interessato veniva chiamato ad acconsentire "in blocco" a un trattamento per finalità promozionali da parte di soggetti terzi non individuati né individuabili. Il Garante ha quindi ritenuto illecito il trattamento fondato su un simile impianto dichiarativo, osservando che la genericità e l'assenza di un'informativa differenziata impediscono l'effettiva comprensione da parte dell'interessato circa l'estensione e la destinazione del trattamento. A supporto di ciò, l'Autorità ha invocato i principi di trasparenza, correttezza e *accountability*, rilevando che la società, pur essendo titolare del trattamento, non aveva approntato misure idonee a dimostrare la legittimità dei consensi raccolti. Tale pronuncia conferma una linea

predefinite: ogni squilibrio informativo mina la sua validità e compromette la legittimità del trattamento ³⁹.

Il caso del modello “*Pay or Consent*”, adottato da alcune grandi piattaforme digitali, è paradigmatico: la pressione economica esercitata sugli utenti affinché acconsentano al trattamento dei loro dati biometrici a fini pubblicitari solleva seri dubbi di compatibilità con il principio di libertà del consenso ⁴⁰. Il parere dell'EDPB del 2024 ha chiarito che tale pratica rischia di configurarsi come una forma di condizionamento indebito, soprattutto nei casi in cui la rinuncia al consenso comporti una perdita economica significativa o una riduzione della qualità del servizio ⁴¹.

La comparazione con altri ordinamenti europei conferma la centralità della questione. In Francia, la CNIL ha vietato il

interpretativa consolidata a livello europeo, secondo cui la libertà del consenso, quale fondamento del trattamento, esige che esso sia espresso in modo autonomo, per ciascuna specifica finalità, in un contesto di piena informazione e assenza di asimmetrie contrattuali o informative. In questa prospettiva, il provvedimento contribuisce a definire i limiti dell'autonomia negoziale nel mercato digitale e rafforza la centralità del soggetto interessato come titolare effettivo dei propri dati personali. Il testo integrale del provvedimento è consultabile al seguente link: « <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10114986> ».

³⁹ La CGUE, nella sentenza *Planet49* (C-673/17, 1 ottobre 2019), ha affrontato con estrema chiarezza il tema del consenso espresso per l'utilizzo dei *cookie* e, più in generale, dei dati personali per finalità commerciali. In quella sede, i giudici di Lussemburgo hanno statuito che il consenso dell'interessato, per ritenersi valido ai sensi della direttiva *ePrivacy* e del GDPR, non può in alcun modo essere desunto da un comportamento passivo dell'utente, come l'uso di caselle preselezionate, né può fondarsi su un'interpretazione meramente presuntiva della volontà dell'interessato. Il consenso, per essere giuridicamente efficace, deve risultare da una manifestazione inequivocabile di volontà, libera, specifica, informata e soprattutto positiva, tale da escludere ogni ambiguità o automatismo. La Corte ha dunque riaffermato che la libertà del consenso implica anche la parità informativa tra le parti, e che qualunque asimmetria informativa o opacità nelle modalità di raccolta rappresenta una violazione dei principi di correttezza e trasparenza, compromettendo la validità dell'intero trattamento. Sebbene la pronuncia si collochi nel contesto della

disciplina dei *cookie*, essa assume una portata sistemica più ampia, poiché definisce i confini essenziali dell'autodeterminazione informativa nel trattamento dei dati personali. Proprio per questo, i principi affermati trovano piena applicazione anche in relazione alla profilazione automatizzata e ai trattamenti biometrici, ove l'esigenza di un consenso libero e consapevole si coniuga con il potenziale impatto intrusivo delle tecnologie impiegate. Per una puntuale disamina della decisione si veda R. CABAZZI, *Utilizzo dei cookie e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di giustizia nel caso Planet49*, in *MediaLaws - Rivista di Diritto dei Media*, 2020, 2, pp. 316 ss.; la stessa viene richiamata, anche se in prospettiva differente, da M.C. MENECHETTI, *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in *MediaLaws - Rivista di Diritto dei Media*, 2021, 1, pp. 266 ss.

⁴⁰ Cfr., V. D'ANTONIO, *Disponibilità del dato personale e nuove declinazioni del principio consensualistico*, in P.G. Monateri (a cura di), *Scritti in memoria di Rodolfo Sacco*, Milano, 2024, pp. 489-508.

⁴¹ Sulla compatibilità dei modelli di fruizione condizionata detti “*Pay or Consent*” con i principi del GDPR, è chiarificatore il Parere n. 08/2024 dell'*European Data Protection Board*, adottato il 17 aprile 2024, in risposta alla richiesta congiunta delle Autorità garanti di Paesi Bassi, Norvegia e del Land tedesco di Amburgo. Il documento prende posizione sulla legittimità del consenso prestato dagli utenti nell'ambito di simili modelli economici, sottolineando la necessità che tale consenso sia autenticamente libero, informato e scevro da condizionamenti economici o asimmetrie informative, ai sensi degli articoli 4, n. 11 e 7 del

riconoscimento facciale per scopi commerciali in spazi pubblici, sostenendo che tale pratica, anche quando non finalizzata all'identificazione in senso stretto, comporta un trattamento invasivo della dimensione corporea, non proporzionato rispetto alla finalità pubblicitaria ⁴².

Una delle decisioni più emblematiche, sul versante europeo, in relazione al trattamento biometrico, questa volta nei contesti di sorveglianza pubblica, è rappresentata dal caso *Bridges*, deciso dalla *Court of Appeal* del Regno Unito nel 2020. In tale occasione, la Corte ha affermato la non conformità all'art. 8 CEDU dell'uso, da parte della polizia gallese, di sistemi di riconoscimento facciale in spazi aperti al pubblico, in assenza di garanzie legislative

Regolamento. Il parere solleva dubbi rilevanti circa l'equilibrio tra accesso ai servizi digitali e tutela dei diritti fondamentali, in particolare quando l'alternativa a un trattamento dati risiede nel pagamento di una somma per la fruizione di contenuti pubblicitari-free. L'*Opinion* 08/2024 dell'EDPB del 17 aprile 2024 è consultabile al seguente link ufficiale: « https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-64/opinion-082024-art-64-opinion-pay-or-consent_en ».

⁴² Nel contesto della crescente diffusione di tecnologie di riconoscimento facciale, il dibattito giuridico ha assunto toni sempre più attenti alle implicazioni che tali strumenti comportano in termini di tutela dei diritti fondamentali. In tale direzione si colloca l'importante intervento del Comitato consultivo della Convenzione 108, che in data 28 gennaio 2021 ha adottato un articolato documento intitolato *Guidelines on Facial Recognition*, con l'intento di offrire un quadro di riferimento normativo e deontologico orientato alla protezione della persona rispetto a trattamenti biometrici automatizzati. Le linee guida, suddivise per destinatari — legislatori, sviluppatori, titolari e responsabili del trattamento — si fondano sul principio che ogni utilizzo del riconoscimento facciale debba essere sottoposto a una valutazione rigorosa in termini di necessità e proporzionalità, tenendo conto non solo della finalità perseguita, ma anche dell'impatto effettivo e potenziale sui diritti e le libertà dell'interessato. In tal senso, viene chiarito che il consenso, ove previsto, non può dirsi valido se ottenuto in contesti di squilibrio informativo o istituzionale, come nel caso delle autorità pubbliche o di soggetti privati incaricati di funzioni analoghe. Particolarmente significativa è la posizione assunta rispetto all'uso del riconoscimento facciale in spazi pubblici e per finalità commerciali: in simili ipotesi, la tecnologia viene ritenuta eccessivamente invasiva della di-

mensione corporea e identitaria della persona, e dunque difficilmente compatibile con il principio di minimizzazione, salvo casi eccezionali e debitamente giustificati. Le linee guida escludono inoltre la liceità dell'impiego del riconoscimento facciale "dal vivo" per finalità promozionali, suggerendo al contrario l'adozione di alternative meno intrusive, quali *badge*, codici o strumenti di autenticazione non biometrici. È proprio su questa stessa linea si colloca la posizione della *Commission Nationale de l'Informatique et des Libertés* (CNIL), che ha più volte espresso riserve in merito all'utilizzo del riconoscimento facciale in spazi aperti al pubblico, in particolare quando destinato a scopi di *marketing* o profilazione comportamentale. La CNIL ha chiarito che, anche in assenza di identificazione nominativa, la mera rilevazione di tratti biometrici finalizzata alla personalizzazione dell'esperienza commerciale costituisce un trattamento altamente invasivo e, in linea di principio, sproporzionato rispetto alla finalità perseguita. In tal senso, la Commissione ha sottolineato la necessità di un'autorizzazione specifica e caso per caso, subordinata alla dimostrazione di garanzie elevate circa l'affidabilità della tecnologia, la protezione dei dati dei minori e la reale possibilità per l'interessato di esercitare un controllo consapevole sul trattamento. Le convergenze tra le raccomandazioni del Comitato della Convenzione 108 e le posizioni adottate dalla CNIL evidenziano la progressiva maturazione di una coscienza giuridica europea volta a contemperare l'innovazione tecnologica con il rispetto dei diritti umani. In particolare, l'uso del riconoscimento facciale emerge come una delle aree in cui la tensione tra efficienza e tutela della persona raggiunge il suo punto più delicato, imponendo ai decisori normativi un approccio fondato su trasparenza, responsabilità e verifica *ex ante* dell'impatto sui diritti. Il riferimento è al Comitato consultivo della Con-

specifiche e sufficientemente precise. La sentenza ha sottolineato l'esigenza che qualunque trattamento automatizzato avente natura identificativa — e ancor più se biometrico — sia sottoposto a stringenti valutazioni di impatto, da svolgersi *ex ante*, e sia giustificato in base a criteri di stretta necessità e proporzionalità.

Di particolare rilievo è, inoltre, l'affermazione per cui l'utilizzo di tecnologie di identificazione biometrica su larga scala, in spazi accessibili alla collettività, esige non solo una disciplina dettagliata ma anche un controllo attivo del potenziale discriminatorio insito negli algoritmi impiegati, in linea con il principio di eguaglianza sostanziale. La pronuncia britannica ha così contribuito, in maniera significativa, a tracciare una soglia di legittimità dell'identificazione biometrica nello spazio pubblico, ponendo il tema dell'*accountability algoritmica* al centro del dibattito sulla legalità dell'innovazione tecnologica ⁴³.

Questi interventi confermano un principio comune: il corpo non è un'interfaccia neutra, e il suo sfruttamento a fini pubblicitari, anche in chiave predittiva o deduttiva, implica un trattamento biometrico pienamente soggetto alle garanzie europee. La profilazione non può mai avvenire in modo silente, né giustificarsi in nome dell'efficienza o della personalizzazione dell'esperienza utente.

Rectius, l'integrazione tra biometria e OBA rappresenta un banco di prova decisivo per il diritto europeo contemporaneo, che è chiamato a proteggere la libertà dell'individuo non solo nella sfera dei dati esplicitamente forniti, ma anche nella dimensione sottile e silenziosa dei dati corporei captati, interpretati e utilizzati per orientare economicamente la volontà del soggetto. È in questa zona grigia, dove la tecnologia supera la soglia della consapevolezza, che il diritto deve esercitare la sua funzione più

venzione 108, *Guidelines on Facial Recognition*, 28 gennaio 2021, disponibile al seguente link: « <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3> ».

⁴³ Il caso *Bridges*, pur non direttamente collegato alla tematica pubblicitaria ma comunque confacente con quella identitaria, ha rappresentato un punto di svolta nella giurisprudenza europea in materia di riconoscimento facciale e protezione dei dati biometrici. La Corte d'Appello inglese (*Court of Appeal of England and Wales*) ha stabilito che l'uso di sistemi di identificazione biometrica remota da parte della polizia gallese — attraverso la tecnologia di *automated facial recognition* (AFR) — ha violato diritti fondamentali sanciti dal *Data Protection Act 2018* (attuativo del GDPR nel Regno Unito), nonché dalla *Human Rights Act 1998*. In particolare, la Corte ha

censurato l'assenza di garanzie *ex ante*, la genericità delle categorie di persone inserite nelle *watchlist* e la sproporzione tra i mezzi impiegati e le finalità di sicurezza pubblica perseguite, evidenziando l'insufficienza del quadro normativo nazionale a tutelare adeguatamente i diritti alla *privacy*, alla protezione dei dati personali e alla libertà di espressione. La decisione ha così riaffermato la necessità di regole chiare, trasparenti e proporzionate per l'uso di tecnologie biometriche in spazi pubblici ad accesso libero, anticipando molti dei principi poi accolti nel testo dell'*AI Act*. Si veda *Court of Appeal (Civil Division), R (on the application of Edward Bridges) v. Chief Constable of South Wales Police*, [2020] EWCA Civ. 1058, sentenza dell'11 agosto 2020, disponibile su: « <https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html> ».

alta: riconoscere e tutelare la dignità dell'umano nella sua espressione più profonda e materiale.

4. BIOMETRIA E VULNERABILITÀ ALGORITMICA: QUANDO IL CORPO DIVENTA FRAGILITÀ ESPOSTA.

L'espansione delle tecnologie biometriche nel trattamento dei dati personali impone, dunque, una riflessione su un aspetto spesso sottovalutato ma giuridicamente cruciale: la vulnerabilità algoritmica⁴⁴. Se è vero, infatti, che ogni individuo può potenzialmente essere soggetto a profilazione o sorveglianza tramite dati biometrici, è altrettanto vero che alcuni soggetti, per la loro condizione personale o sociale, sono maggiormente esposti al rischio di trattamento ingiusto, opaco o discriminatorio.

L'art. 5, par. 1, lett. *a* del GDPR afferma che ogni trattamento deve avvenire « *in modo lecito, corretto e trasparente nei confronti dell'interessato* ». Ma la "correttezza" del trattamento non è un criterio statico: essa dipende dal contesto, dalla posizione dell'interessato, dal grado di consapevolezza, dalla capacità effettiva di autodeterminarsi rispetto alla tecnologia. Ne consegue che la vulnerabilità non è solo un dato sociale, ma una variabile giuridica che influisce sulla valutazione di legittimità del trattamento stesso.

Nel caso dei dati biometrici, la vulnerabilità si manifesta in almeno due direzioni.

Da un lato, esiste una vulnerabilità strutturale, che colpisce minori⁴⁵, anziani, disabili, migranti o persone con limitate competenze digitali. In questi casi, la capacità di comprendere la

⁴⁴ L'espressione vulnerabilità algoritmica designa una forma di esposizione strutturale al rischio che colpisce individui o gruppi sociali allorché le decisioni automatizzate prodotte da sistemi di intelligenza artificiale si basano su *dataset* incompleti, distorti o privi di diversità rappresentativa. Tale vulnerabilità non è meramente tecnica, ma assume una dimensione sistemica e giuridica, poiché compromette il principio di uguaglianza sostanziale e mina l'effettività delle garanzie poste a tutela della dignità e dell'identità personale. Nel contesto del trattamento dei dati biometrici, essa si manifesta attraverso meccanismi di riconoscimento meno accurati nei confronti di categorie sociali minoritarie, rafforzando stereotipi e ampliando le disuguaglianze. Si tratta, dunque, di un rischio che incide non solo sulla correttezza algoritmica, ma sulla tenuta dei principi fondamentali dell'ordinamento giuridico, rendendo necessario un controllo *ex ante* dei modelli predittivi e una vigilanza rafforzata sul *design* delle

tecnologie. È in quest'ottica che si è iniziato a parlare di *algorithmic fairness* come direttrice correttiva, orientata a una progettazione eticamente e giuridicamente consapevole delle architetture digitali. È la dottrina straniera che per lo più si è occupata di *algorithmic fairness*. *Ex multis*, si veda D. HELLMAN, *Measuring algorithmic fairness*, in *Virginia Law Review*, 2020, Vol. 106, 4, pp. 811 ss.; T. B. NACHBAR, *Algorithmic fairness, algorithmic discrimination*, in *Fla. St. U. Law Review*, 2021, Vol. 48, 2, pp. 509 ss.; J. R. BAMBAUER - T. ZARSKY - J. MAYER, *When a Small Change Makes a Big Difference: Algorithmic Fairness Among Similar Individuals*, in *U.C. Davis Law Review*, 2022, Vol. 55, pp. 2337 e spec. 2372; P. HACKER, *Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU Law*, in *Common Market Law Review*, 2018, Vol. 55, 4, pp. 1143-1185.

⁴⁵ L'inarrestabile penetrazione delle tecnologie digitali in ogni ambito della vita

portata del trattamento, di esprimere un consenso libero, o di esercitare i propri diritti è seriamente compromessa, rendendo particolarmente delicato l'uso di tecnologie biometriche. Un sistema di riconoscimento facciale in una scuola, per esempio, può facilmente normalizzare la sorveglianza tra i più giovani, privandoli della possibilità di rifiutare un trattamento che, per sua natura, è continuo e difficilmente percepibile.

Dall'altro lato, esiste una vulnerabilità algoritmica indiretta, che nasce dalle distorsioni insite nei *dataset* su cui si allenano i modelli biometrici. Numerosi studi internazionali hanno dimostrato che algoritmi di riconoscimento facciale possono presentare tassi di errore significativamente più elevati nei confronti di soggetti appartenenti a minoranze etniche, donne, persone non binarie o con disabilità visive ⁴⁶. In tali casi, la discriminazione non è intenzionale, ma tecnicamente incorporata nei meccanismi di apprendimento automatico.

Questo tipo di vulnerabilità pone interrogativi profondi sul principio di non discriminazione (art. 21 della Carta dei diritti

sociale impone una riflessione approfondita, anche sul piano giuridico, circa gli strumenti di tutela da approntare in favore (soprattutto) dei minori nell'ambiente *online*. In quanto soggetti strutturalmente esposti a forme di vulnerabilità acuita, i minori risultano particolarmente esposti ai rischi insiti nell'ecosistema digitale, che spaziano dalla profilazione indebita all'esposizione a contenuti lesivi della loro integrità psicofisica e identitaria, sul punto C. COLAPIETRO - A. IANNUZZI, *I diritti dei minori nella società digitale tra profili di responsabilità ed esigenze di protezione*, in *Rivista di informatica e diritto (RIID)*, 2024, 2, pp. 334 ss.; R. SENICAGLIA, *Rischi identitari per la persona minore d'età nell'ambiente digitale*, in *European Journal of Privacy Law & Technologies (EJPLT)*, 2023, 2, pp. 62 ss. Di contro, argute riflessioni sugli aspetti riguardanti le problematicità della persona umana — anche se non ancora relative alle tematiche digitali — cfr. P. STANZIONE, *Capacità e minore età nella problematica della persona umana*, Camerino-Napoli, 1975, p. 55.

⁴⁶ Si è ormai consolidata, tanto nella dottrina quanto nelle analisi condotte da organismi indipendenti e centri di ricerca, la consapevolezza che i sistemi di intelligenza artificiale — in particolare quelli impiegati per il riconoscimento facciale e la valutazione predittiva — possano produrre effetti discriminatori, anche in assenza di una volontà esplicita o consapevole del programmatore. La radice di tali effetti risiede spesso nella composizione sbilanciata dei

dataset utilizzati per l'addestramento dei modelli, i quali riflettono pregiudizi storici e sociali radicati. Emblematico, in tal senso, è il caso del *software* COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), utilizzato nel sistema giudiziario statunitense per valutare la probabilità di recidiva: studi indipendenti — tra cui quello condotto da ProPublica nel 2016 — hanno evidenziato che l'algoritmo sovrastimava il rischio di recidiva per soggetti afroamericani, sottostimandolo invece per soggetti bianchi a parità di condizioni. Analogamente, studi pubblicati dal MIT Media Lab hanno dimostrato che alcuni sistemi di riconoscimento facciale presentano tassi di errore anche superiori al 30% nel riconoscere correttamente volti di donne con carnagione scura, mentre le percentuali di accuratezza sono decisamente più elevate per uomini caucasici. Tali evidenze dimostrano come l'errore algoritmico possa trasformarsi in una vera e propria distorsione sistemica, con conseguenze dirette sulla dignità, sull'uguaglianza sostanziale e sull'accesso equo a beni e servizi, in violazione del principio di non discriminazione sancito sia a livello europeo (art. 21 della Carta dei diritti fondamentali dell'UE) che costituzionale. In tale prospettiva, la questione del *bias* algoritmico si pone come una delle principali sfide del diritto antidiscriminatorio nell'ecosistema digitale. Il caso è emerso con particolare rilievo giurisprudenziale nella decisione *State of Wisconsin v. Eric L. Lomis*, n. 2015AP157-CR, decisa dalla *Wisconsin Supreme Court* il 13 luglio 2016.

fondamentali dell'UE) e sulla proporzionalità del trattamento. Se un sistema biometrico è più accurato su certi corpi rispetto ad altri, il rischio è che venga naturalizzato un criterio di selezione algoritmica che penalizza proprio coloro che il diritto dovrebbe maggiormente tutelare.

Un approccio giuridico responsabile impone quindi l'adozione di misure differenziate di protezione, in grado di rispondere alla varietà delle situazioni personali. Il GDPR, all'art. 35, prevede l'obbligo di una valutazione d'impatto sulla protezione dei dati (DPIA) per i trattamenti che presentano rischi elevati, tra cui rientrano espressamente i trattamenti biometrici. È qui che il concetto di vulnerabilità deve essere inserito in modo esplicito come criterio di valutazione preventiva, affinché il trattamento sia progettato tenendo conto della possibile asimmetria di potere tra chi tratta e chi subisce il trattamento.

In chiave comparatistica, si segnalano interessanti sviluppi in ordine alla regolamentazione del trattamento dei dati biometrici, in particolare quando riferito a soggetti vulnerabili o a contesti sensibili. In Spagna, l'*Agencia Española de Protección de Datos* (AEPD) si è espressa con fermezza circa i limiti all'impiego di tecnologie biometriche, evidenziando, in un parere del 2019, che l'interesse pubblico non può di per sé giustificare qualsiasi forma di trattamento⁴⁷. L'Autorità ha ribadito che l'utilizzo di strumenti come il riconoscimento facciale, soprattutto all'interno di ambienti educativi, richiede una base giuridica chiara e specifica, in linea con i principi di necessità e proporzionalità sanciti dal GDPR.

In Irlanda, pur in assenza di un provvedimento esplicitamente riferito alla tecnologia di *face recognition* applicata ai minori, rileva comunque la significativa decisione assunta dalla *Data Protection Commission* (DPC) nei confronti di *Instagram*, piattaforma gestita da *Meta*. Con decisione del settembre 2022, la DPC ha comminato una sanzione pari a 405 milioni di euro per il trattamento illecito dei dati personali di utenti adolescenti, cui era consentita la creazione di profili aziendali con visibilità pubblica di indirizzi *email* e numeri telefonici⁴⁸. La pronuncia, pur non

⁴⁷ Trattasi del parere dell'*Agencia Española de Protección de Datos* (AEPD), *Informe jurídico N/REF: 010308/2019*. In questo parere, l'autorità spagnola prende posizione sull'utilizzo del riconoscimento facciale in ambienti scolastici, ritenendo che non sia sufficiente invocare un generico interesse pubblico per giustificare trattamenti di dati biometrici. L'AEPD afferma che tale trattamento necessita di una norma di legge espressa, e deve rispettare i principi di proporzionalità, necessità e minimizzazione,

come previsto dal GDPR. Il parere, seppur non vincolante, ha rappresentato un orientamento significativo per le scuole e le pubbliche amministrazioni spagnole. Per una disamina più approfondita è possibile consultare il seguente link: « <https://www.aepd.es/cs/informes-y-resoluciones/informes-juridicos> ».

⁴⁸ Ancora una volta vale la pena evidenziare una decisione di un'Autorità. *Data Protection Commission* (DPC) — Ireland, *Instagram Decision - Inquiry IN-18-12-2*

incentrandosi sul dato biometrico in senso stretto, richiama un tema essenziale nella materia in esame: la sproporzione tra il livello di comprensione del minore e la complessità dei trattamenti cui è sottoposto, specie quando questi coinvolgano tecnologie invasive come quelle biometriche.

Sul versante canadese, il Commissario per la Privacy ha da tempo evidenziato criticità legate all'adozione di sistemi biometrici da parte delle amministrazioni pubbliche. Sebbene non risulti, ad oggi, un *report* ufficiale specificamente focalizzato sul rischio di "*bias sistemico*", l'Autorità ha in più occasioni sottolineato la necessità che tali tecnologie siano sottoposte a valutazioni *ex ante* capaci di evidenziare i rischi discriminatori, suggerendo l'introduzione di strumenti di controllo come i *fairness test* ⁴⁹. Tali considerazioni risultano tanto più rilevanti se si considera l'impatto che algoritmi biometrici potenzialmente distorti possono produrre su categorie etniche o sociali marginalizzate.

Tali orientamenti convergono su un punto essenziale: la tecnologia non è neutra, e i dati biometrici, proprio perché attingono alla dimensione fisica dell'identità, possono amplificare le disuguaglianze sociali, cognitive e culturali. È dunque necessario adottare un modello di trattamento ispirato al principio di equità algoritmica, che riconosca la diversità dei corpi e delle condizioni, e che non imponga una standardizzazione pericolosa in nome dell'efficienza.

In definitiva, il diritto alla protezione dei dati personali, quando si confronta con la biometria, non può fermarsi a regolare il trattamento, deve comprendere la fragilità dell'umano, tutelarla e rifletterla nei processi di progettazione, implementazione e controllo delle tecnologie. Solo così sarà possibile dare piena attuazione all'art. 1 della Carta dei diritti fondamentali dell'UE: la dignità umana è inviolabile. Anche — e soprattutto — quando incontra l'algoritmo.

(settembre 2022). Con la decisione in commento, l'autorità irlandese ha sanzionato *Instagram* per avere esposto pubblicamente i dati personali (*email* e numeri telefonici) di utenti adolescenti attraverso la gestione di account aziendali. La DPC ha sottolineato che *Meta* non aveva garantito un livello di protezione adeguato al rischio derivante dalla minore età degli utenti, configurando una violazione grave dei principi del GDPR, tra cui trasparenza e protezione dei minori. È possibile consultare sul punto il testo della decisione oggetto di trattazione al seguente *link* di riferimento: « <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry> ».

⁴⁹ Il documento in parola delinea con chiarezza la necessità di sottoporre le tecnologie di riconoscimento facciale a valutazioni preventive di impatto sui diritti fondamentali, con particolare attenzione ai rischi di discriminazione algoritmica. In tale prospettiva, si sollecita l'introduzione di meccanismi di verifica, quali i *fairness test*, soprattutto quando l'utilizzo di sistemi biometrici da parte delle amministrazioni pubbliche possa incidere su gruppi vulnerabili, minoranze etniche o soggetti socialmente marginalizzati. Il *paper* è consultabile al seguente *link* di riferimento, sul sito dell'*Office of the Privacy Commissioner of Canada*: « https://www.priv.gc.ca/en/operations-and-decisions/ar_index/202021/ar_202021/ ».

5. BIOMETRIA PUBBLICA, MUTAMENTO DI FINALITÀ E DOVERE DI RESPONSABILIZZAZIONE: LE SFIDE SISTEMICHE DEL TRATTAMENTO.

Se il trattamento dei dati biometrici nel settore privato solleva questioni complesse legate alla profilazione, alla pubblicità e alla manipolazione delle scelte, non meno rilevanti — anzi, forse ancor più strutturali — sono le implicazioni derivanti dal loro impiego nell'ambito pubblico e nei contesti di sicurezza. È proprio in questi spazi, tradizionalmente caratterizzati da un'elevata discrezionalità e da esigenze di tutela dell'ordine pubblico, che si misura la tenuta costituzionale del sistema della protezione dei dati personali, specialmente quando è in gioco l'identità fisica dell'individuo.

L'utilizzo di sistemi biometrici per il controllo degli accessi in luoghi pubblici, per il monitoraggio dei flussi urbani o per la sorveglianza preventiva in contesti di sicurezza nazionale ⁵⁰ pone interrogativi centrali circa la compatibilità tra le finalità pubblicistiche e il rispetto dei diritti fondamentali, primi fra tutti il diritto alla riservatezza e alla libertà personale. In tali ambiti, la biometria smette di essere uno strumento di autenticazione individuale per divenire tecnologia di categorizzazione e pre-identificazione, talvolta anche inconsapevole, delle persone.

Questa tensione è stata colta con chiarezza dal legislatore europeo, che nel GDPR ha stabilito, all'art. 5, par. 1, lett. b, il principio di limitazione della finalità, in forza del quale i dati personali devono essere raccolti per scopi specifici, espliciti e legittimi, e non possono essere ulteriormente trattati in modo incompatibile con tali finalità originarie ⁵¹. Il dato biometrico, per sua natura, si presta invece a una funzionalità poliedrica e mutevole: può essere inizialmente raccolto per esigenze di accesso sicuro, ma facilmente utilizzato per il monitoraggio degli spostamenti, per l'analisi comportamentale o per scopi investigativi. È proprio questa versatilità che rende la biometria una tecnologia a rischio sistemico: un dato che nasce come garanzia può trasfor-

⁵⁰ Sui sistemi biometrici utilizzati in contesti urbani per la sicurezza nazionale emblematico è l'esempio analizzato in precedenza in relazione al noto caso *Bridges*.

⁵¹ Com'è noto, a norma dell'art. 5, par. 1, lett. b) del Regolamento (UE) 2016/679, i dati personali devono essere trattati nel rispetto del principio di limitazione della finalità, il quale impone che essi siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità. La norma dispone testualmente nella versione inglese ufficiale: « *Personal data shall be: (b) collected for specified, explicit and legitimate purposes and not further processed in a*

manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ». Tale formulazione, volutamente ampia ma precisa, rafforza l'obbligo di coerenza tra le finalità dichiarate e gli scopi effettivamente perseguiti dal titolare del trattamento, rappresentando un argine contro utilizzi secondari non dichiarati, tanto più rilevante quando si tratta di dati biometrici ad alta intensità identificativa.

marsi in strumento di controllo invisibile, sfuggendo ai vincoli originari della raccolta.

Un'ulteriore conferma della centralità dei principi di responsabilizzazione e proporzionalità nell'impiego pubblico di sistemi biometrici proviene dal recente provvedimento del Garante per la protezione dei dati personali dell'11 settembre 2025, concernente il sistema di riconoscimento facciale denominato *FaceBoarding*, implementato presso l'aeroporto di Milano Linate ⁵².

L'Autorità ha condotto un'approfondita istruttoria, richiama espressamente l'*Opinion* 11/2024 dell'EDPB in materia di riconoscimento facciale negli scali aeroportuali, ed ha concluso che il modello adottato da SEA S.p.A. rientrasse nello "Scenario 3" individuato dal Comitato europeo, ossia quello della conservazione centralizzata dei *template* biometrici sotto il controllo del gestore aeroportuale ⁵³.

Tale architettura, secondo il Garante, è incompatibile con i principi di sicurezza, integrità e riservatezza dei dati sanciti dagli artt. 5, par. 1, lett. f), 25 e 32 GDPR, oltre che con il principio di limitazione della conservazione (art. 5, par. 1, lett. e) GDPR), in quanto priva gli interessati di un effettivo potere di controllo esclusivo sui propri dati biometrici e determina un'elevata esposizione al rischio di violazioni massive.

L'Autorità ha inoltre rilevato ulteriori profili di illegittimità:

⁵² Cfr. Garante per la protezione dei dati personali, Provv. 11 settembre 2025, *FaceBoarding* - SEA S.p.A., doc. web n. 10167745. Giova, diffusamente, riportare alcuni passaggi chiave del Provvedimento. L'Autorità accerta che « la soluzione di *FaceBoarding* [...] è pienamente riconducibile allo scenario 3 di cui al Parere dell'EDPB n. 11/2024, e [...] non è pertanto conforme all'art. 5, paragrafo 1, lett. f), e agli articoli 25 e 32 Regolamento »; rileva inoltre che « l'informativa [...] contiene indicazioni inesatte ove riporta che [...] "il modello biometrico [...] resta conservato esclusivamente [nello] smartphone" del passeggero », mentre « il *template* (modello biometrico) è interamente conservato nel sistema centralizzato di SEA [...] e [...] "il *template* biometrico resta conservato esclusivamente nel sistema centralizzato della Società" » (con richiamo ai verbali ispettivi del 7-8 luglio 2025). Si constata, altresì, « la mancata adozione di misure di cifratura del *template* biometrico » (art. 32 GDPR); « tempi di conservazione [...] fino a 12 mesi [...] in contrasto con l'art. 5, par. 1, lett. e), e con l'art. 32 »; nonché che i « varchi « sono di natura ibrida » e « viene comunque generato un *template* biometrico [...] sebbene l'interessato non abbia rila-

sciato il consenso », con « violazione dell'art. 6 » GDPR. Sulla base della gravità delle violazioni, il Garante dispone la « limitazione provvisoria del trattamento » con effetto immediato (atti e motivazione, nonché dispositivo).

⁵³ Sul punto si veda, EDPB, *Opinion* 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and (f), 25 and 32 GDPR), 23 maggio 2024. Il Comitato distingue quattro scenari: (i) Scenario 1 (modello nelle mani dell'interessato): cancellazione dei dati « poco dopo il completamento del confronto » e controllo « sotto l'esclusivo controllo » del passeggero (§§ 38-44); (ii) Scenario 2 (centralizzato ma cifrato, con chiave nota solo all'interessato): compatibile in linea di principio con artt. 5, 25 e 32 sub garanzie, fermo il « periodo di conservazione il più breve possibile » (§§ 53-60, spec. §§ 58-59); (iii) Scenario 3.1 e (iv) Scenario 3.2 (conservazione centralizzata per identificazione, rispettivamente sotto il gestore aeroportuale e sotto la compagnia aerea): non conformi ai principi di necessità e proporzionalità, poiché « l'impatto negativo sui diritti e sulle libertà fondamentali [...] sembra superare il vantaggio previsto » (Scenario 3.1: § 77; Scenario 3.2: § 90; conclusioni §§ 78 e 91).

l'informativa resa agli utenti era fuorviante, poiché affermava che il modello biometrico fosse conservato unicamente sul dispositivo mobile dell'interessato, quando in realtà esso restava nei sistemi centralizzati del gestore aeroportuale, con conseguente violazione dell'art. 13 GDPR; la mancata cifratura dei *template* biometrici integrava una violazione dell'art. 32 GDPR; la conservazione per un periodo fino a dodici mesi in caso di adesione al "programma a lungo termine" risultava sproporzionata rispetto alla finalità dichiarata, in violazione del principio di limitazione della conservazione; infine, i cosiddetti varchi ibridi comportavano la generazione di *template* biometrici anche per passeggeri che non avevano prestato il proprio consenso, con violazione dell'art. 6 GDPR.

Il Provvedimento si colloca in linea di continuità con la posizione espressa dall'EDPB, che aveva ritenuto ammissibili soltanto gli scenari di conservazione decentralizzata (Scenario 1: modello biometrico nelle mani dell'interessato, Scenario 2: modello cifrato centralizzato ma con chiave segreta esclusivamente in possesso del passeggero), e dichiarato non conformi i modelli basati su banche dati centralizzate, siano esse gestite dal gestore aeroportuale o da fornitori *cloud* sotto il controllo delle compagnie aeree.

La decisione del Garante, che ha disposto una limitazione provvisoria e urgente del trattamento, assume rilievo sistemico sotto tre profili: (i) conferma che il principio di *privacy by design e by default* non può ridursi a mero formalismo tecnico, ma deve tradursi in architetture effettivamente rispettose del controllo individuale sul dato; (ii) ribadisce la centralità del criterio di proporzionalità quale parametro sostanziale per valutare la liceità di sistemi biometrici su larga scala⁵⁴; (iii) evidenzia l'importanza di un raccordo tra dimensione nazionale e quadro europeo, poiché l'azione delle Autorità garanti trova fondamento e coerenza nei pareri del Comitato europeo.

In tal senso, la vicenda *FaceBoarding* costituisce un banco di prova paradigmatico per la tenuta del principio di *accountability*, imponendo agli operatori pubblici e privati di adottare modelli organizzativi e tecnici che, oltre a perseguire efficienza ed innovazione, non arrechino un sacrificio ingiustificato ai diritti fondamentali degli interessati.

⁵⁴ Cfr., per un'analisi ancor più puntuale, EDPB, Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, versione 2.0, adottate il 29 gennaio 2020, parr. 88-90, ove si sottolinea che i dati biometrici rientrano tra le categorie particolari di dati ai sensi dell'art. 9 GDPR. L'uso del riconoscimento facciale, specialmente in contesti pubblici, viene indicato

come particolarmente delicato e da valutare con estrema cautela, poiché non può essere giustificato unicamente da ragioni organizzative o di efficienza. Secondo le Linee guida, spetta al titolare dimostrare che la finalità perseguita non sia realizzabile attraverso strumenti alternativi meno invasivi rispetto alla dignità e ai diritti fondamentali degli interessati.

L'esperienza italiana, così delineata, si inserisce in un contesto più ampio, nel quale diverse Autorità di protezione dati europee hanno adottato soluzioni convergenti, tese a contenere i rischi di sorveglianza sistemica insiti nell'uso pubblico delle tecnologie biometriche.

In Francia, già nel 2019, il *Conseil d'État* ha ammonito circa l'uso di tecnologie di riconoscimento facciale nei contesti scolastici, ritenendole sproporzionate rispetto agli scopi perseguiti. In Germania, la Corte Costituzionale federale ha affermato, nella storica sentenza sulla "riservatezza informatica" (*BVerfG 1 BvR 370/07*), che l'identità personale digitale è tutelabile al pari di quella fisica e che il trattamento biometrico in spazi pubblici deve essere strettamente necessario e soggetto a controlli *ex ante* ⁵⁵.

Ancora più esplicita, nel contesto dell'*accountability* pubblica, è la posizione assunta nel Regno Unito dall'*Information Commissioner's Office* (ICO), che ha pubblicato linee guida molto restrittive sul trattamento dei dati biometrici in ambito governativo. In particolare, il *report Biometric Data Guidance* del 2023 ha stabilito che l'utilizzo di dati biometrici per scopi multipli — ad esempio autenticazione e profilazione comportamentale — è ammissibile solo se ciascuna finalità è separatamente identificata, documentata e accompagnata da una base giuridica autonoma, altrimenti si configura un uso indebito per mutamento illecito di finalità ⁵⁶.

⁵⁵ Un significativo contributo, in chiave comparatistica, al delinearsi di un approccio precauzionale nel trattamento dei dati biometrici proviene dalla giurisprudenza francese e tedesca. In Francia, il Tribunale Amministrativo di Marsiglia, con sentenza del 27 febbraio 2020, come già ricordato in precedenza, ha annullato il progetto sperimentale promosso dal Consiglio Regionale della Provenza-Alpi-Costa Azzurra volto all'installazione di tecnologie di riconoscimento facciale in due istituti scolastici. I giudici amministrativi hanno ritenuto che tale misura fosse sproporzionata rispetto alla finalità perseguita — ossia il controllo degli accessi — e non conforme al principio di minimizzazione del trattamento. L'assenza di una base giuridica solida, unita alla difficoltà di assicurare un consenso effettivamente libero da parte degli studenti, ha condotto a una valutazione di illegittimità dell'intervento tecnologico, confermando l'indirizzo della CNIL, già espressasi in senso contrario alla sperimentazione. Parallelamente, in Germania, la Corte Costituzionale Federale, con la celebre sentenza del 27 febbraio 2008 (*BVerfG, 1 BvR 370/07*), ha elevato a diritto fondamentale la garanzia

della riservatezza e dell'integrità dei sistemi informatici, enucleando il principio secondo cui l'identità digitale deve essere tutelata con pari rigore rispetto a quella fisica. La pronuncia, pietra miliare nella giurisprudenza costituzionale tedesca, ha sottolineato la necessità che ogni trattamento automatizzato dei dati, in particolare se effettuato attraverso tecnologie di sorveglianza biometrica in spazi pubblici, sia strettamente necessario, proporzionato e soggetto a stringenti forme di controllo preventivo, al fine di evitare derive intrusive nella sfera più intima della persona. Le due pronunce costituiscono dunque espressione concreta di un orientamento giurisprudenziale teso a riaffermare la primazia della persona rispetto alla logica del controllo, sollecitando una riflessione sull'uso delle tecnologie biometriche nel rispetto dei principi di proporzionalità, trasparenza e legalità.

⁵⁶ Si veda la posizione dell'*Information Commissioner's Office* (d'ora in avanti ICO), "*Consultation on the Draft Biometric Data Guidance*", 18 agosto 2023, disponibile all'indirizzo: « <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-biometric-data->

Negli Stati Uniti, pur in assenza di una normativa federale omogenea, alcuni ordinamenti statali si sono distinti per un'impostazione rigorosa in tema di biometria. In particolare, l'*Illinois Biometric Information Privacy Act* (BIPA)⁵⁷ richiede il consenso informato specifico per ogni trattamento di dati biometrici e prevede responsabilità civile diretta per le violazioni, anche in assenza di danno effettivo. La giurisprudenza statunitense, a partire dal caso *Rosenbach v. Six Flags* (2019), ha ribadito che la raccolta non autorizzata di dati biometrici costituisce una lesione autonoma del diritto alla *privacy*⁵⁸. È interessante osservare come proprio l'obbligo di rendicontazione preventiva (*accountability by design*⁵⁹) sia divenuto, in queste esperienze, un elemento strutturale per la tenuta costituzionale del trattamento.

Sul versante latinoamericano, il Messico ha adottato un impianto normativo peculiare: la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* qualifica i dati biometrici come "sensibili" e impone, anche in ambito pubblico, una valutazione dell'impatto sociale e costituzionale del tratta-

guidance/ ». In questo documento, l'ICO ha delineato linee guida restrittive sul trattamento dei dati biometrici, sottolineando che l'utilizzo per scopi multipli, come autenticazione e profilazione comportamentale, è ammissibile solo se ogni finalità è chiaramente identificata, documentata e supportata da una base giuridica autonoma, altrimenti si configura un uso indebito per mutamento illecito di finalità.

⁵⁷ Il *Biometric Information Privacy Act* (BIPA), adottato dallo Stato dell'Illinois nel 2008, rappresenta uno dei primi e più avanzati esempi di legislazione statale negli Stati Uniti dedicata alla tutela dei dati biometrici. La norma impone agli enti privati l'obbligo di ottenere un consenso informato, esplicito e scritto prima di raccogliere, conservare o divulgare dati biometrici — quali impronte digitali, scansioni del volto o della retina — e stabilisce rigorosi requisiti in materia di conservazione, sicurezza e distruzione dei dati. Particolarmente rilevante è la previsione dell'azione civile privata (*private right of action*), che consente agli interessati di agire in giudizio per la violazione della legge, contribuendo a generare una significativagiurisprudenza applicativa. Questo modello normativo ha posto le basi per una protezione avanzata dei diritti individuali nel contesto digitale e ha ispirato numerose proposte legislative in altri Stati federati americani.

⁵⁸ La Suprema Corte dell'Illinois, con la nota decisione *Rosenbach v. Six Flags Entertainment Corp.*, ha inaugurato un

orientamento interpretativo di grande rilevanza sistemica in materia di tutela dei dati biometrici, chiarendo che la semplice raccolta non autorizzata di tali dati — senza necessità di un danno ulteriore o conseguenze materiali tangibili — è già di per sé sufficiente a costituire una violazione del diritto alla *privacy*, ai sensi del *Biometric Information Privacy Act*. La Corte ha infatti stabilito che la lesione del diritto alla riservatezza si configura nel momento stesso in cui un soggetto acquisisce o conserva dati biometrici senza aver rispettato i requisiti formali di informazione e consenso previsti dalla normativa. Tale pronuncia ha avuto un impatto rilevante nel consolidare l'idea secondo cui la titolarità del dato biometrico è elemento costitutivo dell'identità personale, e che ogni trattamento effettuato in assenza di base giuridica valida compromette in radice l'autodeterminazione informativa dell'individuo, anche in assenza di danni economici immediatamente percepibili. Per consultare analiticamente la decisione si rinvia a *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, 129 N.E.3d 1197 (Ill. 2019). Testo completo della decisione: « <https://www.illinoiscourts.gov/Resources/f71510f1-fb2a-43d8-ba14-292c8009dfd9/123186.pdf> ».

⁵⁹ Così, N. SCHÖNHERR - H. VOGL-PÖSCHL - F. FINDLER - A. MARTINUZZI, *Accountability by design? Exploring design characteristics of corporate social responsibility standards*, in *Sustainability Accounting, Management and Policy Journal* (SAMPJ), 2021, Vol. 13, 1, pp. 2 ss.

mento, con particolare attenzione agli effetti sulle minoranze e sulle comunità indigene⁶⁰. Una lettura che si avvicina alla prospettiva di una protezione “differenziata” e attenta alla vulnerabilità sistemica, di cui anche il diritto europeo sembra progressivamente farsi carico.

In questo scenario, assume rilievo centrale il principio di *accountability* (art. 5, par. 2 GDPR), che impone al titolare del trattamento, come ampiamente noto, non solo di rispettare i principi generali, ma di essere in grado di dimostrarlo attivamente, attraverso documentazione, procedure e valutazioni *ex ante*. Il dovere di responsabilizzazione non è, dunque, un mero onere procedurale, ma una forma nuova e sostanziale di presidio giuridico, che richiede un cambio di paradigma: dal trattamento come atto tecnico, alla *governance* del dato come processo etico e legale insieme⁶¹.

Rectius, il cardine operativo dell'*accountability* è rappresentato, dall'art. 24 GDPR, che impone al titolare l'obbligo di implementare misure tecniche e organizzative adeguate, anche in funzione della natura dei dati trattati. Quando si tratta di dati biometrici, e a maggior ragione in ambito pubblico, tali misure devono assumere una forma rafforzata: valutazioni d'impatto, minimizzazione delle finalità, trasparenza, sistemi di *audit* indipendenti. Non è sufficiente che il trattamento sia astrattamente lecito; è necessario che l'intera architettura organizzativa del titolare sia improntata a una cultura della protezione, capace di prevenire gli abusi prima ancora che sanzionarli.

La biometria, in questo quadro, diventa cartina di tornasole della responsabilità pubblica: laddove essa viene trattata con leggerezza, flessibilità o senza rigore finalistico, si apre la strada a una compressione silenziosa ma persistente dei diritti fondamentali. È necessario, allora, riconoscere che il dato biometrico non è un semplice strumento tecnico, ma un bene informativo ad

⁶⁰ In Messico, la protezione dei dati biometrici trova un fondamento esplicito nella *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (LFPDPPP), pubblicata nel *Diario Oficial de la Federación* il 5 luglio 2010. La normativa qualifica espressamente i dati biometrici come “sensibili” (art. 3, lett. VI), assoggettandoli a un regime rafforzato di tutela, il quale impone — anche nel settore pubblico, in base a successive disposizioni normative e interpretative — un’attenta valutazione dell’impatto del trattamento, con specifico riguardo alle implicazioni costituzionali e sociali. Particolare attenzione è riservata agli effetti su categorie vulnerabili, tra cui le minoranze etniche e le comu-

nità indigene, in coerenza con il principio *pro persona* sancito dalla Costituzione messicana all’art. 1.

Per il testo della legge si veda il sito ufficiale del *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* (INAI).

⁶¹ Con specifico riferimento alla *governance* dei dati, risulta quanto mai attuale riferirsi alla Sez. 2, denominata “Requisiti per i sistemi di IA ad alto rischio”, *Sub. art. 10*, della già menzionata opera di A. MANTELEO - G. RESTA - G.M. RICCIO (a cura di), *Intelligenza artificiale. Commentario. Regolamento (UE) 2024/1689 - AI ACT Linee guida Commissione europea pratiche vietate Disegno di legge sull'intelligenza artificiale*, op. cit., spec. pp. 223 ss.

altissima densità identitaria, e come tale deve essere gestito con una consapevolezza giuridica che non si limiti alla conformità formale, ma si estenda alla qualità sostanziale della legittimità.

Solo un approccio profondamente responsabile, finalistico e proporzionato può impedire che la versatilità del dato si traduca in ambiguità normativa e, in ultima analisi, in deriva autoritaria del trattamento. In gioco non vi è soltanto la protezione del dato, ma la struttura stessa del rapporto tra potere pubblico e individuo, tra trasparenza istituzionale e libertà personale.

6. L'ILLUSIONE DELL'ANONIMIZZAZIONE E IL RISCHIO PERSISTENTE DI RE-IDENTIFICAZIONE NEI DATI BIOMETRICI.

Tra le sfide più profonde e trasversali legate al trattamento dei dati biometrici si colloca quella del rischio di re-identificazione, che si manifesta anche — e forse soprattutto — quando il dato è sottoposto a operazioni di anonimizzazione o pseudonimizzazione⁶². È proprio la tensione tra apparente neutralizzazione del dato e residua potenzialità identificativa a rendere la biometria un campo giuridicamente fragile, in cui l'equilibrio tra sicurezza e identità è costantemente esposto alla frizione dell'evoluzione tecnologica.

Il principio, formalmente chiaro, è noto: i dati resi anonimi in modo irreversibile escono dal perimetro applicativo del GDPR. Tuttavia, nel contesto dei dati biometrici, l'anonimizzazione risulta spesso illusoria, poiché la struttura stessa del dato, fondata su caratteristiche uniche, stabili e non modificabili della persona, conserva tracce persistenti di identità. Anche in assenza di un nome, di un codice identificativo diretto o di un dato anagrafico esplicito, l'identità rimane latente, potenzialmente rievocabile

⁶² Per re-identificazione si intende, com'è noto, il processo mediante il quale un dato personale, previamente sottoposto a tecniche di anonimizzazione o pseudonimizzazione, viene nuovamente associato, direttamente o indirettamente, a un interessato identificabile. Tale possibilità evidenzia il carattere spesso solo apparente dell'anonimato e impone una riflessione critica sul livello effettivo di protezione che operazioni tecniche di minimizzazione dei rischi possono offrire. Sotto il profilo giuridico, la re-identificazione rappresenta una vulnerabilità strutturale del trattamento, in quanto riattiva la riconducibilità del dato a una persona fisica, con tutte le conseguenze in termini di applicabilità del GDPR. In tal senso, è particolarmente rilevante l'orientamento dell'EDPB, secondo cui la valuta-

zione del rischio di re-identificazione deve essere concreta, realistica e contestualizzata, tenendo conto dei mezzi "ragionevolmente utilizzabili" da parte del titolare o di terzi per risalire all'identità dell'interessato (cfr. Parere n. 05/2014 del WP29 e Linee guida 4/2019 sull'anonimizzazione). Ne consegue che anche un dato pseudonimizzato, se trattato in un contesto che consente la re-identificazione, non può essere considerato anonimo ai fini dell'esclusione dell'ambito applicativo della disciplina sulla protezione dei dati personali. Sul concetto di re-identificazione si veda M. VIOLA DE AZEVEDO CUNHA - D. DONEDA DANILO - N. ANDRADE, *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, in *Cib. e dir.*, 2010, Vol. 11, 4, pp. 641-655.

attraverso strumenti di inferenza, correlazione e ricostruzione computazionale.

In particolare, si sono affermate nel tempo tecniche di cosiddetto *reverse engineering* identitario⁶³, capaci di risalire all'identità di un soggetto a partire da dati apparentemente de-identificati. Tali tecniche si fondano sulla possibilità di ricostruire tratti biometrici da modelli codificati — come vettorializzazioni facciali, impronte vocali o tracciati comportamentali — e di incrociarli con fonti ausiliarie, come archivi pubblici, metadati di localizzazione, interazioni sociali digitali o persino banche dati sanitarie⁶⁴ e commerciali. Ciò consente, con l'ausilio di sistemi di intelligenza artificiale addestrati su grandi volumi di dati, di individuare connessioni significative che possono condurre a un'identificazione sufficientemente precisa del soggetto, pur in assenza di dati formalmente personali.

In questo scenario, anche i dati biometrici pseudonimizzati, o

⁶³ Il *reverse engineering* identitario consiste in un insieme di tecniche che consentono di risalire all'identità di un soggetto a partire da dati apparentemente anonimi o pseudonimizzati, tramite la decodifica di modelli biometrici o la combinazione di diverse fonti ausiliarie. Tale pratica si fonda sulla possibilità, sempre più concreta grazie alle capacità computazionali dell'intelligenza artificiale, di ricostruire tratti fisici o comportamentali — come volti, impronte vocali, andature, segnature neurali o schemi d'interazione digitale — da rappresentazioni vettoriali, set di dati intermedi o *pattern* di comportamento. Il fenomeno, in diversi ambiti, è stato oggetto di studi da parte di P. SAMUELSON - S. SCOTCHMER, *The Law and Economics of Reverse Engineering*, in *Yale Law Journal*, 2001-2002, Vol. 111, pp. 1575 ss. e spec. 1630 ss.; e ancora, M. BIRNACK, *Reverse Engineering Informational Privacy Law*, in *Yale J.L. & Tech.*, 2012, Vol. 15, pp. 24 ss.

⁶⁴ Tra i più insidiosi terreni di applicazione delle tecniche di re-identificazione vi è indubbiamente quello rappresentato dalle banche dati sanitarie, che — pur costituendo un irrinunciabile patrimonio per la ricerca clinica, epidemiologica e farmacogenomica — espongono i soggetti interessati a rischi di profilazione altamente invasiva. Le banche dati sanitarie, infatti, raccolgono informazioni estremamente sensibili, spesso strutturate in forma pseudonimizzata o codificata, ma non sempre effettivamente anonime. In tale contesto, la ricostruzione identitaria può avvenire per correlazione, sfruttando l'interoperabilità tra *dataset* biometrici e sanitari attraverso metodi computazionali avanzati, in grado di agganciare —

anche indirettamente — un dato clinico a un'identità fisica. Numerosi studi di settore hanno dimostrato come, partendo da modelli biometrici derivati da immagini facciali, segnali vocali o tracce digitali comportamentali, sia possibile risalire alla persona cui essi appartengono incrociandoli con *dataset* sanitari aperti o scarsamente protetti. In particolare, è stata evidenziata la vulnerabilità di archivi contenenti dati genomici o radiologici (ad es. TAC, risonanze, PET), i quali — se non adeguatamente anonimizzati — possono essere combinati con sistemi di riconoscimento facciale tridimensionale o con strumenti di classificazione morfologica basati su intelligenza artificiale. Questo scenario pone in discussione la tenuta stessa del principio di anonimizzazione come garanzia assoluta di non identificabilità, imponendo una riflessione critica sulla validità delle misure tecniche e organizzative adottate, ai sensi dell'art. 32 del GDPR. Inoltre, la possibilità che l'incrocio tra dati biometrici e sanitari venga sfruttato da attori privati per fini non compatibili con la finalità originaria del trattamento — si pensi, ad esempio, all'ambito assicurativo o occupazionale — richiama in modo stringente l'esigenza di un rafforzamento delle tutele, in linea con i principi di finalità, minimizzazione e integrità sanciti dal Regolamento. Come già sottolineato in più occasioni dal Comitato europeo per la protezione dei dati e dallo stesso Garante italiano, la de-identificazione non può essere considerata una misura statica, bensì un processo dinamico, il cui grado di efficacia va periodicamente riesaminato alla luce dell'evoluzione tecnologica e della crescente disponibilità di banche dati accessorie. Per argute argomen-

trattati in forma dichiaratamente anonimizzata, si espongono a un rischio concreto di re-identificazione, in particolare negli ambienti ad alta densità informativa. È proprio in ragione di questa vulnerabilità intrinseca che il Parere n. 01/2025 dell'*European Data Protection Board*, pubblicato il 28 febbraio 2025, ha affermato con chiarezza che la pseudonimizzazione, pur essendo una misura raccomandabile in chiave di *accountability*, non può mai essere equiparata all'anonimizzazione, né tantomeno far venir meno l'applicabilità del GDPR⁶⁵. In particolare, l'EDPB sottolinea che, nel caso dei dati biometrici, la pseudonimizzazione non neutralizza la potenzialità identificativa, ma la sospende temporaneamente, in modo del tutto contingente rispetto al contesto, alle tecnologie disponibili e alla presenza di informazioni supplementari.

La problematicità è aggravata dal fatto che i dati biometrici non sono modificabili: una volta compromessi, non possono essere rigenerati o sostituiti. A differenza delle credenziali digitali, essi non sono revocabili. L'individuo non può cambiare il proprio volto, la propria impronta digitale o la propria mappa vocale. Di conseguenza, la compromissione di un dato biometrico genera un rischio strutturalmente permanente, difficilmente sanabile anche attraverso tecniche evolute di mitigazione.

Da qui discende una seconda riflessione di ordine sistemico: l'inadeguatezza delle sole misure tecniche di protezione in assenza di presidi normativi sostanziali, coerenti e lungimiranti⁶⁶. Il trattamento di dati biometrici non può essere affidato esclusivamente alla robustezza crittografica di un'infrastruttura, o alla raffinatezza algoritmica di un sistema di mascheramento. Occorre, piuttosto, che l'ordinamento giuridico eserciti una funzione anticipatoria, definendo uno statuto autonomo del dato biome-

tazione sul trattamento dei dati sanitari, *ex multis*, si veda F. DI CIOMMO, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp.*, 2002, 2, pp. 121 ss.; C. PERLINGIERI, *eHealth and Data*, in R. Senigaglia - C. Irti - A. Bernes (eds.), *Privacy and data protection in software services*, New York, 2021, pp. 127 ss.; G. FINOCCHIARO - L. GRECO, *Trattamento di dati sanitari per la ricerca scientifica: nuove prospettive*, in *Diritto Mercato Tecnologia (DIMIT)*, 2024, pp. 1 ss.

⁶⁵ Sul punto, si veda *European Data Protection Board (EDPB), Guidelines 01/2025 on Pseudonymisation*, adottate il 16 gennaio 2025 e sottoposte a consultazione pubblica. Il documento chiarisce che la pseudonimizzazione costituisce una misura tecnica utile ai fini dell'*accountability*, ma non equivale in alcun modo all'anonimizza-

zione, né elide l'applicabilità del GDPR ai sensi dell'art. 4, n. 5 del Regolamento. Le Linee guida sono consultabili al seguente indirizzo: « https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf ».

⁶⁶ Sul punto, si veda 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.it*, 2024, 28, pp. 91 ss., dove l'Autrice approfondisce il tema dei presidi a tutela dei diritti fondamentali nelle ipotesi di sorveglianza derivanti dall'uso della biometria, rilevando come, in assenza di un quadro normativo organico e sostanziale, la protezione dell'individuo si fondi, prevalentemente su strumenti tecnici, non sempre idonei a garantire una salvaguardia effettiva e lungimirante.

trico come elemento di identità strutturale, e non semplicemente come dato “sensibile” in senso classico.

Ne consegue, anzitutto, l'esigenza di una limitazione chiara e precisa delle finalità ammissibili per il trattamento, in ossequio al principio di specificità di cui all'art. 5, par. 1, lett. *b* del GDPR. A ciò si aggiunge l'obbligo, per i titolari del trattamento, di svolgere valutazioni d'impatto rafforzate, che non si limitino alla misurazione del rischio tecnico, ma tengano conto anche del potenziale effetto sociale, psicologico e relazionale della possibile re-identificazione. A livello organizzativo, il principio di *accountability*, sancito dall'art. 24 del GDPR, impone un modello di gestione del rischio che superi la mera conformità documentale, e si traduca in un effettivo governo del ciclo di vita del dato biometricamente rilevante.

Apertis verbis, il dato biometricamente trasformato non smette di essere identità. La sua decontestualizzazione non ne annulla la forza identificativa, ma ne differisce l'attivazione. Ed è proprio questo potenziale identificativo latente che il diritto deve presidiare con rigore. Anonimizzare, in ambito biometrico, non significa cancellare, ma solo dissimulare. E quando la dissimulazione si fonda su presupposti tecnologici instabili, la garanzia giuridica rischia di trasformarsi in una promessa fragile. L'identità, allora, non si protegge attraverso strumenti illusori, ma con un impianto normativo solido, orientato alla prevenzione e alla minimizzazione dell'esposizione. È in questo spazio che la biometria si rivela non solo come oggetto di trattamento, ma come banco di prova della tenuta della nostra concezione giuridica della persona.

7. RIFLESSIONI CONCLUSIVE. RESTARE LIBERI, NONOSTANTE IL DATO.

Il percorso argomentativo tracciato ha avuto come orizzonte costante l'interrogativo sulla compatibilità tra l'evoluzione tecnologica legata alla biometria e la tenuta del sistema dei diritti fondamentali, nel quadro normativo europeo contemporaneo ⁶⁷. È emerso, con chiarezza crescente, che il dato biometrico non è un dato come gli altri, ma un elemento dotato di specialissima densità identitaria, che racchiude in sé il corpo, la storia e la vulnerabilità della persona.

A differenza di altri dati personali, i dati biometrici non si limitano a “rappresentare” l'individuo: lo incarnano. Ne descrivono l'unicità in modo non replicabile, ne proiettano i tratti corporei all'interno di architetture digitali che li trasformano in

⁶⁷ In tema di compatibilità tra evoluzione tecnologica e diritti fondamentali, alla luce delle strategie unionali, cfr. A. ADINOLFI, *Evoluzione tecnologica e tutela dei*

diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione, in *Quaderni AISDUE*, Sezione “Atti convegni AISDUE”, 2023, 15, pp. 321 ss.

chiavi di accesso, strumenti di riconoscimento, modelli predittivi. In questo processo, la corporeità viene computata, segmentata, astratta e resa oggetto di trattamento automatizzato. È qui che il diritto incontra una sfida di ordine non solo normativo, ma culturale e assiologico: la persona rischia di diventare funzione, il volto parametro, il corpo codice.

Si è analizzato come la profilazione, quando alimentata da dati biometrici, assuma una qualità nuova e particolarmente problematica. Essa cessa di essere una semplice ricostruzione statistica delle preferenze dell'utente per diventare un'anticipazione comportamentale fondata sull'identità fisica stessa. Le espressioni del volto, l'andatura, la postura, il tono della voce non sono più semplicemente osservati, ma interpretati, categorizzati e impiegati per orientare decisioni, preferenze, scelte economiche. Il dato biometrico diviene così veicolo di influenza commerciale, discriminazione automatizzata, o sorveglianza predittiva.

In questo contesto, il diritto alla protezione dei dati personali si mostra nella sua dimensione più profonda: non come semplice strumento di controllo documentale, ma come presidio giuridico della libertà, della dignità e dell'integrità della persona. La sfida, tuttavia, è resa più complessa dalla natura ambigua e poliedrica del dato biometrico, il quale, una volta raccolto, può facilmente essere riutilizzato, reinterpretato, trasferito, con effetti che travalicano le finalità originarie. È in questo slittamento funzionale che si annidano i pericoli più gravi, soprattutto quando il trattamento avviene al di fuori di una consapevolezza piena da parte dell'interessato.

L'analisi ha messo in luce l'insufficienza delle misure tecniche — pur necessarie — se non accompagnate da presidi normativi chiari, finalizzati e proporzionati. La pseudonimizzazione, l'uso di algoritmi sicuri, la cifratura, non possono da sole garantire una reale tutela, soprattutto se il contesto operativo è opaco o se il rischio di re-identificazione è strutturalmente connaturato alla natura del dato trattato. È qui che il diritto è chiamato ad esercitare la propria funzione regolativa più alta: non inseguire la tecnologia, ma governarla, restituendo centralità alla persona ⁶⁸ anche nei contesti più automatizzati.

La ricognizione svolta ha anche evidenziato come l'*accountability*, intesa come dovere di responsabilizzazione piena da parte del titolare del trattamento, debba tradursi in una cultura giuridica del limite, del rispetto e della vigilanza preventiva. Non si tratta

⁶⁸ Sulla centralità della persona umana e sul necessario controllo in relazione agli strumenti tecnologici — in particolare quelli di IA — si rimanda ad A. PROCIDA MIRABELLI DI LAURO, *Le intelligenze artificiali tra re-*

sponsabilità civile e sicurezza sociale, in P. Perlingieri - S. Gioia - I. Prisco (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Napoli, 2020, pp. 297 ss.

di moltiplicare adempimenti formali, ma di edificare architetture giuridiche trasparenti, verificabili, coerenti con la dignità dell'umano.

A fronte di tali dinamiche, volendo porre una provocazione, sembrerebbe opportuno interrogarsi su nuove categorie giuridiche che possano arricchire il catalogo dei diritti fondamentali: dal diritto alla non manipolazione algoritmica, al diritto alla neutralità biometrica, fino alla tutela dell'integrità cognitiva e relazionale nel contesto dell'intelligenza artificiale. In tale prospettiva, si colloca anche il recente dibattito intorno ai cosiddetti neurodiritti, ovvero quei diritti emergenti che mirano a proteggere la libertà mentale, l'identità neuronale e l'autonomia cognitiva dell'individuo di fronte alle tecnologie capaci di leggere o influenzare l'attività cerebrale. Sebbene i dati biometrici, nella loro configurazione attuale, non rientrino direttamente nell'ambito delle neurotecnologie, essi condividono con queste ultime una tensione comune: la possibilità che l'identità personale venga progressivamente ridotta a oggetto di trattamento automatizzato, con effetti potenzialmente manipolativi o invasivi. La riflessione sui neurodiritti, allora, si presenta come specchio teorico utile a rafforzare, per analogia, la consapevolezza giuridica della necessità di proteggere non solo il dato, ma la persona nella sua interezza fisica, comportamentale e cognitiva ⁶⁹.

In conclusione, dall'insieme delle argomentazioni esposte emerge chiaramente che il trattamento dei dati biometrici, soprattutto quando finalizzato alla profilazione, rappresenta una delle sfide più delicate e sistemiche per il diritto dell'informazione contem-

⁶⁹ Particolarmente significative, in tale prospettiva, sono le riflessioni di P. Stanzone, secondo cui l'avvento delle neurotecnologie impone una riconsiderazione profonda del rapporto tra persona e dato, nella misura in cui l'elaborazione algoritmica della mente — mediante tecniche di *brain-reading* o interventi potenzialmente manipolativi del processo cognitivo — rischia di vulnerare direttamente la libertà di autodeterminazione individuale. Se l'impiego terapeutico di tali dispositivi, ad esempio per contrastare patologie neurodegenerative, appare pienamente auspicabile, più problematico è l'uso a fini di potenziamento cognitivo o di profilazione del comportamento mentale, che solleva questioni inedite di natura etica, giuridica e antropologica. La riflessione del Presidente dell'Autorità Garante della Privacy ruota attorno all'idea di un necessario riconoscimento dei neurodiritti come presidio di garanzia dell'integrità neuropsicologica della persona, intesa non soltanto come soggetto di dati, ma come tito-

lare di uno spazio interiore insuscettibile di interferenze esterne. Una simile prospettiva, pur ancorata al dominio delle neuroscienze, si rivela di cruciale importanza anche nella disciplina dei dati biometrici, nella misura in cui questi — se trattati con finalità di riconoscimento, categorizzazione o previsione comportamentale — possono finire per intaccare la dimensione più profonda dell'identità personale. La necessità di tutelare il foro interno quale sede di formazione libera e autonoma del pensiero si presenta, dunque, come principio guida per orientare la disciplina delle tecnologie emergenti, non solo sul piano della *privacy*, ma in una più ampia visione costituzionale della dignità umana. Si veda sul punto P. STANZONE, *Neurodiritti, la libertà e i confini della scienza*, in *Corriere della Sera*, 2021, intervento pubblicato in occasione della Giornata europea della protezione dei dati personali, rinvenibile al link: « <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/>

poraneo. Il compito del giurista, oggi, non è solo quello di interpretare le norme esistenti, ma di preparare il campo normativo per ciò che ancora non è completamente visibile, ma già pienamente operante.

In gioco non vi è soltanto il controllo sul dato, ma la possibilità per l'individuo di restare libero, nonostante il dato. E questa, in definitiva, è la più alta missione che il diritto possa oggi assumere.

Abstract

Il contributo si propone di analizzare il tema del trattamento dei dati biometrici nel contesto della profilazione algoritmica, esaminandone le implicazioni normative, etiche e sistemiche alla luce del GDPR e dell'*AI Act*. A partire dall'analisi della definizione giuridica di dato biometrico e del suo legame con le tecniche di riconoscimento automatizzato, lo studio si sofferma sulla funzione di questi dati nell'ambito della pubblicità comportamentale, evidenziando il rischio di pratiche manipolative e l'emergere di nuove forme di vulnerabilità algoritmica. Particolare attenzione è riservata all'uso dei dati biometrici nel settore pubblico, alla problematica del mutamento di finalità e all'insufficienza delle sole misure tecniche di protezione in assenza di presidi giuridici sostanziali. Sullo sfondo dell'intera trattazione si sviluppa un confronto con esperienze normative e giurisprudenziali di altri ordinamenti, volto ad arricchire la prospettiva interpretativa in chiave comparata. Il saggio si conclude con una riflessione teorica sulla necessità di un ripensamento delle categorie giuridiche tradizionali, in vista della possibile affermazione di nuovi diritti

9527386 ». Ancora, per una lettura comparata sul tema dei neurodiritti, merita particolare attenzione il caso cileno, primo ordinamento a introdurre un riconoscimento costituzionale esplicito della necessità di proteggere l'attività cerebrale come dimensione inviolabile della persona. Con l'emendamento approvato nel 2021, il Cile ha affermato il principio secondo cui i dati neurali, intesi come espressione dell'identità cognitiva individuale, devono essere sottratti a ogni forma di commercializzazione o trattamento privo di un consenso effettivo, fondando così un nucleo di tutele innovative che si proiettano oltre la tradizionale disciplina della *privacy*. Emblematico in tal senso il caso deciso dalla Corte Suprema cilena nel 2023, che ha accolto il ricorso di un ex parlamentare contro l'uso di un dispositivo di neuro-monitoraggio in grado di acquisire informazioni cerebrali, ritenendo la raccolta dei dati non conforme ai principi co-

stituzionali e disponendone la cancellazione. La vicenda ha rappresentato un banco di prova concreto per l'applicazione giurisprudenziale dei neurodiritti, confermandone la portata come presidio avanzato a tutela della libertà cognitiva. Pur nella consapevolezza di talune perplessità dottrinali circa la sovrapposizione con altri diritti fondamentali già previsti — come la dignità, la libertà personale e la riservatezza — l'esperienza cilena costituisce un riferimento normativo significativo, ispirato a una visione della persona centrata sulla integrità neuropsichica e sulla protezione del foro interno da ogni forma di manipolazione algoritmica o interferenza esterna. Proprio sulla tematica dei *neurorights* e *mental privacy*, con riferimento al caso cileno si veda V. D'ANTONIO - G. SICA, *Neurodiritti e mental privacy: alla ricerca di un framework normativo*, in V. D'Antonio (a cura di), *Diritti digitali*, Nocera Inferiore (SA), 2023, pp. 293 ss. e spec. 313.

fondamentali, quali la neutralità biometrica, la non manipolazione algoritmica e la tutela dell'integrità cognitiva della persona nell'ecosistema digitale.

This paper aims to analyze the issue of biometric data processing within the framework of algorithmic profiling, exploring its legal, ethical, and systemic implications under the GDPR and the AI Act. Starting from the legal definition of biometric data and its connection to automated recognition technologies, the study focuses on the role such data plays in behavioural advertising, highlighting the risk of manipulative practices and the emergence of new forms of algorithmic vulnerability. Special attention is paid to the use of biometric data in the public sector, the issue of purpose drift, and the insufficiency of technical safeguards in the absence of substantive legal guarantees. Throughout the paper, a comparative approach is adopted by referencing selected legal and jurisprudential experiences from other jurisdictions, with the aim of enriching the interpretive framework. The paper concludes with a theoretical reflection on the need to reconsider traditional legal categories and to recognize the possible emergence of new fundamental rights, such as biometric neutrality, protection against algorithmic manipulation, and the safeguarding of cognitive integrity in the digital ecosystem.