federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

25 MARZO 2026

Riconoscimento facciale: tecnologie che corrono, diritti che frenano. Il caso italiano del *Faceboarding*

di Matteo Bottari
Segretario generale e Data Protection Officer
Comune di Rho

ed Elettra Currao
Expert giuridico
Banca d'Italia

Riconoscimento facciale: tecnologie che corrono, diritti che frenano. Il caso italiano del *Faceboarding* *

di Matteo Bottari
Segretario generale e Data Protection Officer
Comune di Rho

ed Elettra Currao
Expert giuridico
Banca d'Italia

Abstract [It]: Il contributo esamina in chiave comparata i diversi approcci regolatori al riconoscimento facciale, state driven, market driven e rights driven, evidenziandone le asimmetrie derivanti dal bilanciamento tra sicurezza, mercato e diritti. Analizza, inoltre, l'interazione tra GDPR e AI Act, il regime dei dati biometrici, tra sovrapposizioni e tensioni interpretative, e il recente provvedimento del Garante sul Faceboarding di Milano Linate, sottolineando la necessità di un quadro armonizzato che concili innovazione e tutela dell'autodeterminazione informativa.

Title: Facial recognition: technologies that race ahead, rights that hold back. The Italian case of Faceboarding
Abstract [En]: The paper provides a comparative analysis of regulatory approaches to facial recognition, state-driven, market-driven, and rights-driven, highlighting asymmetries between security, market interests, and individual rights. It discusses the complex interaction between the GDPR and the AI Act, examines the Italian Data Protection Authority's recent prohibition of Faceboarding at Milan Linate Airport, and emphasizes the need for a harmonized framework that balances technological innovation with the protection of informational self-determination.

Parole chiave: Riconoscimento facciale, dati biometrici, intelligenza artificiale, protezione dei dati personali, Garante privacy, faceboarding
Keywords: Facial Recognition, biometric data, artificiale intelligence, data protection, faceboarding

1. Introduzione

Il tema del riconoscimento facciale (*facial recognition technology*: FRT) continua a suscitare ampi dibattiti in tutto il mondo. Questa tecnologia si è evoluta in maniera esponenziale rispetto alle prime sperimentazioni risalenti a qualche decennio fa[1]. Oggi, lo sviluppo di strumenti sempre più sofisticati di estrazione ed elaborazione di informazioni dalle immagini di volti umani gestiti dall'intelligenza artificiale con il *machine*

* Articolo sottoposto a referaggio. Si precisa, in modo inequivocabile, che le opinioni espresse non impegnano la responsabilità degli Enti di appartenenza né rappresentano posizioni ufficiali degli stessi, riflettendo esclusivamente le opinioni degli Autori.

[1] Si tratta delle indagini svolte da Woody Bledsoe per conto della *Central Intelligence Agency* (CIA) americana. Nel 1963 Bledsoe pubblicò il primo di due rapporti dal titolo "*Proposta di studio per determinare la fattibilità di una macchina per riconoscimento facciale semplificato*". Negli stessi anni, due scienziati di Harvard, David Hubel e Torsten Wiesel, lavoravano a una ricerca che avrebbe gettato le fondamenta della *computer vision* odierna.

learning e il *deep learning*, accompagnato dalla disponibilità di *big data*[2], ovvero di un flusso costante di immagini raccolte anche grazie all'ascesa delle piattaforme social che rendono l'IA sempre più accurata, ha reso le tecnologie biometriche particolarmente diffuse e, in alcuni casi, invasive. Questo avviene a causa dell'acquisizione e del controllo di dati anche in contesti molto intimi, estendendo i problemi (etici, giuridici, ecc.) ben oltre una semplice questione di privacy e arrivando a toccare ambiti quali l'autonomia, la possibilità di azione individuale e l'autodeterminazione.

Proprio alla luce di tali sviluppi, negli ultimi anni, complice anche il fatto che i sistemi di identificazione facciale hanno il vantaggio di non essere 'invasivi' tanto quanto altri metodi di riconoscimento biometrico (quali occhi, impronte digitali) e che possono essere alimentati da immagini acquisite anche senza il consenso degli interessati nel momento in cui gli stessi le mettono a disposizione sui vari social media, il volto umano ha assunto un estremo rilievo e le tecnologie di *facial recognition* hanno subìto un notevole impulso di crescita, estendendosi in un ambito di ricerca più vasto concernente l'intelligenza artificiale (IA)[3].

Tuttavia, rispetto ad altri campi di sviluppo dell'IA, quello del riconoscimento facciale denota una maggiore difficoltà operativa a seconda della prospettiva sociopolitica entro la quale viene inquadrato.

2. Diversi approcci nell'uso del riconoscimento facciale: *state driven*, *market driven* e *rights driven*

Muovendo da questa premessa, pur nella consapevolezza che ogni ricostruzione teorica di modelli differenti sul tema FRT possa rivelarsi forzata e troppo rigida per ricomprendere in un unicum concettuale le diverse tipologie tecniche utilizzate per gli scopi più vari, si ritiene, però, possibile

[2] Sui recenti successi del *deep learning* dovuti, più che a innovazioni rivoluzionarie nell'ambito dell'IA, alla disponibilità di quantità immense di dati, ci si permette di rinviare a M. BOTTARI, E. CURRAO *Regolamentazione e governance dell'intelligenza artificiale nelle smart cities: metodi e strumenti per un approccio utile e sicuro,* in AziendaItalia, n. 3/2024, pp. 393-405.

[3] Per la più recente dottrina in materia si rinvia a: E. SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, 2025; G. SCIANCALEPORE *Riconoscimento facciale e dati biometrici. Una prima riflessione*, 2024, Iura And Legal System, vol. n. 11 p. 44 ss.; G. MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; in ambito anglosassone: NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, National Academies Press, 2024; P. DAUVERGNE, *Identified, Tracked, and Profiled. The Politics of Resisting Facial Re-cognition Technology*, 2022. Tra i rapporti commissionati da Istituzioni internazionali: FRA-EU AGENCY FOR FUNDAMENTAL RIGHTS *Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2019,* D. DUSHI *The use of facial recognition technology in EU law enforcement: Fundamental rights implications, in Policy Brief,* 2020, qui consultabile, EUROPEAN PARLIAMENT, *Regulating facial recognition in the EU,* EPRS settembre 2021, WORLD ECONOMIC FORUM, *A Policy Framework for responsible limits on facial recognition use case: law enforcement investigations,* settembre 2021; in particolare, per le Istituzioni statunitensi: CONGRESSIONAL RESEARCH SERVICE, *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations, R46541,* settembre 2020; U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses, GAO-20-522,* agosto 2020.

un'illustrazione 'tripartita'. Una simile impostazione, consentendo di schematizzare le ragioni che dettano l'uso nei diversi sistemi socio-politici in cui le tecnologie vengono applicate, può dimostrarsi rivelatrice di una coerenza di fondo. Tale coerenza caratterizza i diversi sistemi di governo.

Secondo la ricostruzione di Bradford, sarebbe possibile distinguere, almeno, tre distinti approcci: state driven, market driven e rights driven[4].

In una prospettiva c.d. *state driven* adottata in Paesi come Cina, Russia e in altri Stati autoritari, la tecnologia di riconoscimento facciale viene usata in maniera capillare spesso con la finalità di effettuare controlli penetranti negli ambiti più diversi della vita sociale e individuale. Si arriva a servirsene per reprimere sistematicamente il dissenso politico[5] e per il monitoraggio sistematico della popolazione.

Emblematico, sotto questo profilo, è il caso della Cina, ove, nonostante la recente approvazione del Codice Civile (2020) il cui articolo 1035 stabilisce i principi generali di protezione dei dati, come le limitazioni di scopo e ambito, nonché l'obbligo del consenso informato da parte degli interessati nel trattamento dei dati personali, seguita a ruota dalla legge sulla *Privacy* (*Personal Information Protection Law* – del 2021), continua a permanere un quadro giuridico molto asimmetrico in base al quale se il riconoscimento facciale viene utilizzato dal settore pubblico non è soggetto alle particolari limitazioni, cui, invece, è soggetto nell'ambito privato. Il governo (centrale o locale) può sempre giustificare un uso pervasivo del riconoscimento facciale ai fini della sicurezza pubblica basandosi sul principio che la raccolta e l'analisi dei dati debbano essere attivamente coltivate per rafforzare la capacità dello Stato di raggiungere un'ampia gamma di obiettivi di '*governance* sociale'.

Così è stato possibile giustificare un uso altamente invasivo di questa tecnologia da parte della *Beijing Subway Limited Company* (la metropolitana di Pechino). Durante la pandemia, il governo municipale di Pechino ha implementato un sistema di IA in base al quale i dati facciali dei passeggeri della metropolitana sarebbero stati collegati ai risultati delle vaccinazioni e dei tamponi Covid-19 e, da maggio 2022, il sistema è stato ulteriormente rafforzato con un aggancio al "codice sanitario" cinese, l'applicazione mobile utilizzata dai cinesi per i controlli obbligatori sui dati di localizzazione e sui referti sanitari. Negli ultimi anni, sempre sulla linea di garantire la massima sicurezza, diverse amministrazioni locali cinesi hanno

[4] Si fa riferimento alle tre prospettive *state driven*, *market driven* e *rights driven* analizzate da A. BRADFORD, *Digital Empires*, in *Oxford University Press*, 2023, pp.6 e segg.

[5] In una delle sue ultime pronunce contro la Russia, la Corte Europea dei Diritti dell'Uomo di Strasburgo ha, infatti, stabilito che l'arresto e la successiva sanzione amministrativa inflitta al ricorrente, reo di aver condotto una protesta individuale e pacifica e, in seguito, identificato dalle forze di pubblica sicurezza tramite sistemi biometrici di riconoscimento facciale, costituisce una violazione del diritto alla vita privata, ex art. 8 CEDU18, nonché una illegittima compressione della libera manifestazione del pensiero protetta dall'art. 10 della Convenzione Corte EDU, (GLUKHIN C. RUSSIA, Terza Sezione, n. 11519/20, 4 luglio 2023, sulla quale si veda: C. NARDOCCI, *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU Glukhin c. Russia,* in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2024, pp. 279 e ss.). Sulla situazione in Cina, in generale, *Come la Cina usa l'intelligenza artificiale per controllare gli Uiguri*, in "Sole 24ore", 15/04/2019.

imposto agli hotel (privati) di verificare l'identità dei propri ospiti installando sistemi FRT collegati al *database* della polizia e scansionando i loro volti al momento del *check-in*[6].

In generale, la prospettiva *state driven* comporta un quadro normativo più permissivo per quanto riguarda l'uso della tecnologia di riconoscimento facciale. Le normative sono meno severe (soprattutto rispetto alla diversa prospettiva *rights driven* tipicamente europea), consentendo un'implementazione più ampia della tecnologia in vari settori, inclusa la sorveglianza pubblica, senza gli stessi requisiti di consenso e trasparenza o, comunque, di rispetto dei diritti fondamentali. Esistono poche restrizioni legali alla raccolta e all'utilizzo dei dati biometrici, il che lascia alle autorità un ampio margine di manovra per implementare il riconoscimento facciale senza una supervisione o una responsabilità significative[7].

Negli Stati Uniti si privilegia un modello *market driven*, basato sulla fiducia nelle dinamiche spontanee del mercato per favorire il benessere economico e sociale. In questo contesto, la libertà di espressione, di informazione e l'iniziativa economica privata incontrano il minor numero possibile di ostacoli. L'intervento delle autorità pubbliche è quindi limitato al minimo indispensabile per assicurare la sicurezza nazionale e il regolare funzionamento del mercato.

Un esempio paradigmatico, a questo proposito, è quello della piattaforma *Clearview AI*[8].

Clearview AI (utilizzata solo negli Stati Uniti, ma non in altri Paesi di *Common Law* come il Regno Unito, il Canada e l'Australia) offre un *database* di immagini del volto e un motore di riconoscimento facciale: gli operatori delle forze dell'ordine possono caricare una 'foto soggetto' e ottenere corrispondenze potenziali da un archivio costruito con immagini reperite *online*[9]. L'azienda dichiara che la sua tecnologia viene usata solo dalle forze dell'ordine e dalle agenzie governative e principalmente 'a posteriori' (cioè, dopo che un episodio è avvenuto) per investigazioni, e non in tempo reale su larga scala[10].

Nonostante la dichiarazione aziendale, ci sono segnalazioni di un uso massiccio di FRT da parte di numerosi dipartimenti di polizia (circa 1/6 di tutte le forze di polizia statunitensi) e di circa un milione di

---

[6] Cfr. J-A. LEE, P. ZHOU, *FRT regulation in China*, in *The Cambridge Handbook of Facial Recognition in the Modern State* 2024 Cambridge University Press, pp. 242 e segg. Per ulteriori approfondimenti M. BICCHIRI, *Asia e intelligenza artificiale. Strategie, regolamentazione e sfide globali*, in *La Nuova Giurisprudenza Civile Commentata*, n. 3/2025, p. 798

[7] I. VIRTUOSO, LI CHEN *Navigating face recognition technology: a comparative study of regulatory and ethical challenges in China and the European Union,* in (a cura di) C. VRABIE**,** *Machine Intelligence, 2024, pag.111-140.*

[8] *Clearview AI* è un motore di ricerca basato sul riconoscimento facciale. Il sistema di sorveglianza sviluppato dalla società statunitense raccoglie, mediante tecniche di *web scraping*, immagini provenienti da *social network*, *blog* e, in generale, da siti *web* che rendono pubblicamente accessibili foto o video. Le immagini così acquisite vengono poi elaborate tramite tecniche biometriche per estrarne le caratteristiche identificative, generando modelli (*template*) biometrici che, nella fase di ricerca, vengono confrontati con l'immagine oggetto dell'interrogazione, dando luogo a un processo di verifica.

[9] Si parla di un *database* di oltre 60 miliardi di immagini pubbliche.

[10] In pratica, gli agenti delle forze dell'ordine con un *account Clearview AI* possono utilizzare un computer o uno *smartphone* per caricare la foto di un individuo sconosciuto sul sistema di riconoscimento facciale di *Clearview AI*. Il sistema (a pagamento) può restituire risultati di ricerca che mostrano potenziali foto dell'individuo conosciuto, nonché *link* ai siti da cui sono state ottenute le foto (ad esempio, *Facebook*).

ricerche fatte tramite *Clearview AI* negli USA. Una recente indagine del *Washington Post*[11] ha rivelato che le forze dell'ordine statunitensi stanno utilizzando gli strumenti di intelligenza artificiale in un modo per cui non avrebbero mai dovuto essere utilizzati: come scorciatoia per trovare e arrestare i sospettati senza altre prove.

L'Unione europea ha scelto un modello *rights driven*, volto principalmente a proteggere i diritti delle persone dai rischi legati alle tecnologie digitali. Diversamente dal modello *market driven* che limita l'intervento pubblico per non ostacolare la libertà economica e di informazione, quello europeo considera l'azione dei pubblici poteri indispensabile non solo per garantire queste libertà, ma anche per bilanciarle con gli altri diritti fondamentali, a partire dalla tutela dei dati personali. Sebbene condivida con il modello *state driven* l'idea di un intervento pubblico, il modello europeo si differenzia perché il ruolo dello Stato non è controllare i cittadini, ma assicurare la protezione dei loro diritti cercando di bilanciare il diritto alla libertà di espressione con una serie di altri diritti fondamentali quali la dignità umana e il diritto alla *privacy*. Questo approccio ha reso necessaria l'adozione di una regolamentazione estesa e articolata.

Per questi motivi, nei Paesi in cui il modello regolatorio è *rights driven*, una tecnologia di IA come quella offerta da *Clearview* ha subito parecchie restrizioni, quando non la messa al bando. Infatti, l'uso di tale tecnologia nell'UE risulta oggi fortemente contrastato: l'*European Data Protection Board* (EDPB) ha dichiarato che «l'uso di un servizio quale *Clearview AI* da parte di autorità di polizia dell'Unione Europea non sarebbe, allo stato, conforme al regime UE di protezione dei dati». Le Autorità dei vari paesi europei (tra cui il Garante per la protezione dei dati personali in Italia) hanno avviato indagini e sanzionato *Clearview* per violazioni del regolamento generale sulla protezione dei dati (GDPR)[12].

[11] D. MACMILLAN, D. OVALLE, A. SCHAFFER, *Arrested by AI: Police ignore standards after facial recognition matches* in *The Washington Post*, 13.01.2025, qui consultabile.

[12] *Clearview AI* risulta, ad oggi, vietata in molti Paesi europei (Svezia, Italia, Regno Unito, Grecia, Francia, Paesi bassi): con specifico riferimento all'istruttoria e al conseguente provvedimento adottato dal Garante italiano nei confronti della società statunitense è emerso che il sistema predisposto da *Clearview AI*, diversamente da quanto affermato dalla società, consentiva il tracciamento anche di cittadini italiani e di persone collocate in Italia. In particolare, è emerso che i dati personali detenuti dalla società, inclusi quelli biometrici e di geolocalizzazione, venivano trattati illecitamente, senza un'adeguata base giuridica. La società violava inoltre altri principi base del Regolamento UE sulla privacy, come quelli relativi agli obblighi di trasparenza, non avendo adeguatamente informato gli utenti, di limitazione delle finalità del trattamento, avendo utilizzato i dati degli utenti per scopi diversi rispetto a quelli per i quali erano stati pubblicati online e di limitazione della conservazione, non avendo stabilito tempi di conservazione dei dati. La società è stata dunque sanzionata dal Garante, che ha disposto altresì la cancellazione dei dati relativi a persone che si trovano in Italia e ne ha vietato l'ulteriore raccolta e trattamento attraverso il suo sistema di riconoscimento facciale. Per approfondimenti si rinvia a D. BIANCHI, *Clearview bannato anche dal Garante della Privacy olandese*, in *Diritto e Giustizia*, 2024, qui consultabile e E. CADAMURO, *Le nuove sfide per la tutela penale dei dati biometrici nella costruzione dell'identità digitale: tra istanze europee e sistema nazionale*, in *Rivista Trimestrale di Diritto Penale dell'Economia*, n. 3-4/2024, p. 364.

3. Le tecnologie di riconoscimento facciale al vaglio della normativa europea e nazionale sulla protezione dei dati personali

Il modello *rights driven* europeo non si esaurisce in una presa di posizione teorica, ma trova una traduzione concreta in un articolato impianto normativo, volto a governare preventivamente i rischi connessi all'uso delle tecnologie di riconoscimento facciale.

Il legislatore dell'Unione europea muove dalla convinzione che, nel campo dell'intelligenza artificiale, la tutela dei diritti fondamentali non possa essere affidata soltanto alle dinamiche di mercato o a interventi correttivi successivi. Per questa ragione, nell'ambito delle tecnologie di riconoscimento facciale si è ritenuto necessario introdurre una disciplina preventiva, idonea a incidere sulle fasi di progettazione, addestramento e controllo dei sistemi. Tale scelta riflette il superamento di una visione basata su un'alternativa rigida tra efficienza e protezione dei diritti. Un'impostazione esclusivamente orientata all'innovazione avrebbe infatti condotto a una regolazione minimale, mentre un approccio incentrato solo sulla tutela dei diritti avrebbe giustificato forme di controllo eccessivamente invasive. L'Unione europea ha pertanto adottato una soluzione mediata, volta a conciliare lo sviluppo tecnologico con la salvaguardia dei diritti fondamentali.

Il differente approccio rispetto agli altri modelli (*state driven* e *market driven*) è anche il frutto del diverso impatto della normativa in materia di protezione dei dati personali negli ordinamenti europei e della sempre più crescente difficoltà nell'armonizzare tali disposizioni con quelle di recente elaborazione in materia di Intelligenza Artificiale, anche con riguardo al tema del riconoscimento facciale.

L'utilizzo di tecnologie di riconoscimento facciale determina, infatti, un trattamento di dati biometrici rientranti nella categoria di dati personali c.d. particolari cui è accordata una protezione rafforzata ai sensi dell'articolo 9 GDPR[13].

L'utilizzo di tecniche di riconoscimento facciale tramite il trattamento di dati biometrici comporta maggiori rischi per i diritti e le libertà degli interessati e, in particolare, rischi di usi impropri (falsi negativi, distorsioni e discriminazione), fino ai casi più gravi di usurpazione d'identità o impersonificazione. È per questo che, prima di utilizzare tali tecnologie, i titolari del trattamento dovrebbero valutare l'impatto sui diritti e sulle libertà fondamentali degli interessati e considerare se mezzi meno invasivi possano

[13] Come anche chiarito dall'EPDB nelle Linee guida 3/2019 dell'EDPB sui dispositivi video, versione 2.0, 29 gennaio 2020, punto 74 (qui consultabili) dati quali le caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, e che siano oggetto di misurazione, sono qualificabili come "dati biometrici" 13. Infatti, l'immagine di un volto di una persona (una fotografia o un video), anche detto "campione" biometrico, consente di estrarre una rappresentazione digitale (c.d. "modello") delle caratteristiche distintive di tale volto13. La conservazione di tale campione in una banca dati biometrica consente l'identificazione univoca dell'interessato ed eventualmente può essere usata per l'autenticazione del soggetto. Il risultato dell'identificazione è il risultato dell'applicazione di tecniche probabilistiche con le quali verificare la corrispondenza tra il modello confrontato e quello di riferimento contenuto nella banca dati. Se dunque la probabilità supera un determinato valore soglia predeterminato dallo sviluppatore o dall'utente utilizzatore il sistema fornirà l'esito dell'identificazione e/o autenticazione.

raggiungere la finalità legittima del trattamento[14]; è, inoltre, fondamentale una chiara e precisa informazione dell'interessato sulle modalità e sui rischi connessi al trattamento ed è preferibile fondare tali trattamenti sulla base giuridica del consenso, a condizione che esso sia libero e sempre revocabile[15].

Per queste ragioni, il GDPR prevede che qualsiasi trattamento con tali caratteristiche dovrà essere preceduto da una Valutazione di impatto sulla protezione dei dati personali (art. 35) ad esito della quale, qualora permanga un rischio residuo elevato per i diritti e le libertà degli interessati, dovrà essere chiesto un parere preventivo di legittimità all'Autorità Garante. Queste tutele sono necessarie affinché il trattamento sia conforme ai principi basilari che reggono la materia della protezione dei dati personali: legittimità, proporzionalità, necessità, minimizzazione dei dati, *privacy by design* e *privacy by default*.

La disciplina del GDPR va combinata con quella prevista nel Regolamento sull'Intelligenza Artificiale dell'Unione Europea (AI Act[16]), ove i sistemi di riconoscimento facciale occupano una posizione centrale, in quanto ritenuti tra le applicazioni di intelligenza artificiale più invasive rispetto ai diritti fondamentali della persona, avendo ad oggetto trattamenti relativi a dati biometrici[17]. Il legislatore europeo li colloca

[14] A ciò si aggiunga che il legislatore italiano, con il d.lgs. n. 101/2018, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio", ha introdotto nel D.lgs. n. 196/2003 l'art. 2-septies. Tale norma stabilisce che i dati biometrici, possono essere oggetto di trattamento solo quando ricorre una delle condizioni previste dal paragrafo 2 dell'art. 9 del Regolamento e nel rispetto delle misure di garanzia stabilite dal Garante mediante apposito provvedimento. Si consideri, inoltre, quanto previsto, già in precedenza, dal d.lgs. 18 maggio 2018, n. 51, attuativo della direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti in materia penale, il quale include tra i dati personali anche quelli biometrici. Per questi ultimi, così come per quelli genetici, è prevista una consultazione preventiva del Garante prima del trattamento, trattandosi di operazioni che comportano un rischio elevato per i diritti e le libertà degli interessati (art. 24, comma 1, lett. b).

[15] La posizione assunta dal Garante privacy italiano sembra essere quella per cui l'unica base giuridica utilizzabile sia quella del consenso ex art. 6, lett. a) "non esistendo al momento alcuna norma che consenta l'uso di dati biometrici, come prevede il Regolamento, per svolgere una tale attività." (cfr. Provvedimenti nn. 105, 106, 107, 108 e 109 del 22 febbraio 2024 e Provvedimento n. 338 del 6 giugno 2024). Tuttavia, nell'ambito del trattamento dei dati biometrici nel contesto lavorativo il Garante ha precisato che "alla luce della asimmetria tra le rispettive parti del rapporto di lavoro e la conseguente, eventuale, necessità di accertare, di volta in volta e in concreto, l'effettiva libertà della manifestazione di volontà del dipendente, il consenso non costituisce, di regola, un valido presupposto di liceità per il trattamento dei dati personali in ambito lavorativo, indipendentemente dalla natura pubblica o privata del datore di lavoro (cons. n. 43; art. 4, punto 11), e art. 7, par. 3 e 4, del Regolamento" (cfr. Provvedimento n. 167 del 27 marzo 2025). L'Autorità sembra così escludere in toto il trattamento dei dati biometrici nel contesto lavorativo non essendovi, ad oggi, una base giuridica del trattamento né potendo quest'ultima essere rappresentata dal consenso del lavoratore.

[16] Regolamento (UE) 2024/1689, approvato il 13 marzo 2024.

[17] Sul punto si veda anche il considerando n. 15 dell'AI Act "La nozione di «identificazione biometrica» di cui al presente regolamento dovrebbe essere definita come il riconoscimento automatico di caratteristiche fisiche, fisiologiche e comportamentali di una persona, quali il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti, allo scopo di determinare l'identità di una persona confrontando i suoi dati biometrici con quelli di altri individui memorizzati in una banca dati di riferimento, indipendentemente dal fatto che la persona abbia fornito il proprio consenso. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali." Le disposizioni previste dall'AI Act vietano, tra le altre cose, l'uso di sistemi di identificazione biometrica a distanza in tempo reale in spazi pubblici da parte delle forze dell'ordine, salvo condizioni molto restrittive (autorizzazione giudiziaria o amministrativa, limitazione temporale/spaziale).

prevalentemente nella categoria dei sistemi di IA ad alto rischio[18], sottoponendoli a un regime giuridico particolarmente rigoroso.

L'AI Act introduce un divieto generale dell'uso di sistemi di riconoscimento biometrico remoto in tempo reale negli spazi accessibili al pubblico, soprattutto quando tali sistemi sono impiegati dalle autorità di contrasto proprio per evitare forme di sorveglianza di massa, ammettendo solo circoscritte eccezioni[19]. Diversamente, i sistemi di riconoscimento facciale impiegati in modalità non in tempo reale, ossia su immagini o registrazioni già acquisite, non sono oggetto di un divieto assoluto, ma rientrano comunque nella categoria dei sistemi ad alto rischio. Per tali applicazioni, l'AI Act impone una serie di obblighi stringenti volti a garantire affidabilità, sicurezza e tutela dei diritti fondamentali, prescrivendo specifici requisiti tecnici che assicurino la qualità dei modelli algoritmici e la robustezza tecnica dei modelli di IA[20]. Infine, il regolamento prevede un divieto di utilizzo di sistemi di categorizzazione biometrica finalizzati a individuare particolari categorie di dati (come l'origine etnica, le convinzioni religiose e politiche, l'orientamento sessuale), in quanto una simile finalità si pone in contrasto con i valori fondamentali dell'Unione o col sistema di garanzie fondamentali sancito dalla Carta dei diritti fondamentali dell'UE.

Il rapporto tra AI Act e il GDPR è di complementarità sistematica, non di sovrapposizione o sostituzione. Infatti, le due normative operano su piani diversi ma coordinati, concorrendo alla costruzione di un quadro unitario di tutela dei diritti fondamentali nell'ecosistema digitale europeo: il GDPR tutela il dato personale e l'individuo come interessato, il secondo governa il rischio tecnologico dell'IA[21]. Sul punto, uno studio molto recente ha approfondito le interazioni tra l'AI Act e il GDPR, evidenziando come queste due normative, pur perseguendo obiettivi legittimi e complementari, generino una serie di

[18] Il Regolamento adotta un *risk-based approach* che classifica i sistemi di intelligenza artificiale in quattro livelli di rischio determinati in base al loro utilizzo: definite in relazione alle modalità di impiego del sistema: (i) rischio inaccettabile; (ii) rischio elevato; (iii) rischio ridotto o minimo; (iv) rischio connesso a specifici obblighi di trasparenza. A ciascuna categoria corrispondono obblighi e limitazioni proporzionati al potenziale impatto sui singoli e sulla società. Secondo alcuni Autori tale impostazione rischia di essere messa a dura prova dalla velocità dell'evoluzione dei sistemi di IA rispetto alla quale una valutazione solo ex ante (senza un giudizio anche a valle) crea rischi di sovrastima o sottovalutazione della pericolosità. G. LO SAPIO, L'Artificial Intelligence Act e la prova di resistenza per la legalità algoritmica, in federalismi.it, n. 16/2024

[19] Cfr. considerando n. 33 del Regolamento "L'uso di tali sistemi a fini di attività di contrasto dovrebbe pertanto essere vietato, eccezion fatta per le situazioni elencate in modo esaustivo e definite rigorosamente, nelle quali l'uso è strettamente necessario per perseguire un interesse pubblico rilevante, la cui importanza prevale sui rischi. Tali situazioni comprendono la ricerca di determinate vittime di reato, comprese le persone scomparse, determinate minacce per la vita o l'incolumità fisica delle persone fisiche o un attacco terroristico nonché la localizzazione o l'identificazione degli autori o dei sospettati di reati elencati nell'allegato del presente regolamento"

[20] L'AI act prevede obblighi sia in capo ai produttori che agli utilizzatori (Sezione II, artt. 9 e ss.), tra cui la Valutazione di conformità e di impatto sui diritti fondamentali, monitoraggio e segnalazione, obblighi di trasparenza.

[21] F. DONATI, *La protezione dei diritti fondamentali nel regolamento sull'intelligenza artificiale*, in *AIC-Rivista dell'Associazione italiana dei Costituzionalisti*, n. 1/2025, qui consultabile. Secondo l'Autore «l'AI Act offre una tutela di carattere "orizzontale", che non sostituisce ma si aggiunge a quella di cui i diritti e le libertà fondamentali già dispongono in forza del vigente quadro normativo».

sovrapposizioni, tensioni e ambiguità[22] che complicano la conformità per gli operatori, in particolare per chi sviluppa o utilizza sistemi di intelligenza artificiale[23].

In questo contesto il ruolo del Garante privacy italiano nella tutela dei diritti digitali a fronte di simili trattamenti è stato sempre di primo piano. Sin dai primi tentativi di applicazione delle tecnologie d'intelligenza artificiale ai dati personali, il Garante ha compreso il rischio rappresentato dall'esposizione delle persone fisiche (e delle loro vite) a processi di decisione automatizzata basati sulla lettura e l'elaborazione algoritmica di dati[24].

In particolare, i primi provvedimenti del Garante in tema di trattamento di dati biometrici risalgono a diversi anni prima dell'entrata in vigore del GDPR. Infatti, già nel 2001 il Garante si pronunciava in tema di sistemi di videosorveglianza che prevedevano il trattamento di dati biometrici, fissando – in via del tutto eccezionale e in attesa di un intervento sistematico del legislatore - alcune condizioni per consentirne una temporanea installazione all'interno degli istituti di credito nel rispetto di alcune imprescindibili garanzie per gli interessati[25]. Inoltre, nel 2012 il Garante adottava le "Linee-guida in materia di

[22] Sul punto si veda P. FALLETTA, A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Rivista italiana di informatica e diritto*, n. 1/2024, pp. 119 e ss. «Considerati gli ampi margini di potenziale sovrapposizione, l'attuazione delle due discipline potrebbe portare ad un eccesso di regolamentazione. Per questo motivo, il rapporto simbiotico tra protezione dei dati personali e intelligenza artificiale deve porsi al centro dell'esame e della relativa attuazione dell'AI Act, al fine di prevenire eventuali contrasti o contrapposizioni con la disciplina complementare del GDPR […] il fenomeno dell'*over-regulation* è sempre un'arma a doppio taglio, nella misura in cui, se è vero che garantisce l'esistenza di più normative che da fronti diversi proteggono gli stessi diritti, dall'altro, se non ben regolato, rischia di ottenere l'effetto opposto alla finalità iniziale, mettendo a rischio quegli stessi diritti che si prefiggeva di tutelare». Si veda anche E. RAFFIOTTA, *Dalla self-regulation alla over-regulation in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in Osservatoriosullefonti.it, n. 2/23, pp. 245 e ss. L'Autore parla di vero e proprio "assillo normativo" del legislatore europeo mosso dall'intento di costruire «un ecosistema digitale orientato alla tutela individuale, attraverso la predisposizione di adeguate garanzie a protezione dei cittadini (nonché consumatori e fruitori dei servizi digitali cui tali norme si riferiscono). Ciononostante, il lodevole intento che muove il legislatore europeo non può - esso solo - ritenersi bastevole a elidere le evidenti criticità insite in tale modus operandi».

[23] Tra i punti di maggiore disallineamento viene evidenziato l'ambito dei diritti degli interessati (es. accesso, rettifica, cancellazione) il cui esercizio, nell'ambito dei modelli IA, diventa tecnicamente difficile, se non impossibile. Analogamente, l'AI Act prevede ambienti di test controllati (c.d. sandbox) ma non esonero dal rispetto del GDPR. Ciò si traduce, essenzialmente, in un ostacolo all'utilizzo di tali sistemi, anche in fase di sperimentazione, per lo più nel caso di utilizzo di dati sensibili. Per ulteriori approfondimenti si rinvia allo studio commissionato dal Parlamento Europeo (Comitato ITRE) dal titolo "*Interplay between the AI Act and the EU digital legislative framework*", ottobre 2025.

[24] Ancora prima dell'entrata in vigore del GDPR, il Garante aveva già esaminato e censurato trattamenti fondati sull'analisi delle condotte di navigazione degli utenti di siti commerciali, nonché sistemi di valutazione reputazionale basati su attività di *data scraping online*, finalizzati all'attribuzione di punteggi e alla formazione di classifiche relative agli interessati (Provvedimento del 26 luglio 2018, doc. web. n. 9052099 - Metavaluate). Tali interventi evidenziavano l'emersione di un principio che sarebbe stato successivamente formalizzato dall'art. 22 del GDPR, riconoscendo all'interessato il diritto di non essere sottoposto a decisioni assunte unicamente mediante trattamenti automatizzati, compresa la profilazione, idonei a produrre effetti giuridici o comunque significativamente incidenti sulla sua sfera personale. Degne di nota sono, infine, le posizioni assunte dall'Autorità in relazione all'uso di sistemi di intelligenza artificiale nel contesto universitario, con particolare riferimento agli esami a distanza (Provvedimento del 16 settembre 2021, doc. web n. 9703988 - Proctoring Bocconi), nonché nel settore lavorativo (Provvedimento del 13 novembre 2024, doc. web n. 10074601 – Foodinho Glovo).

[25] Provvedimento del 28 settembre 2001, doc. web n. 39704.

riconoscimento biometrico e firma grafometrica"[26] ove si precisava la necessità che il trattamento dei dati biometrici si svolgesse in conformità alle disposizioni del Codice e ai principi di liceità, necessità, finalità e proporzionalità, e a condizione che non si determini un'ingerenza ingiustificata e sproporzionata nei confronti degli interessati.

Nei più recenti provvedimenti il Garante ha diffusamente affrontato il tema della protezione dei dati personali nell'ambito dell'utilizzo dei sistemi di riconoscimento facciale[27]. In generale, il Garante ha ritenuto in plurime occasioni non legittimo l'uso delle tecniche di riconoscimento facciale in quanto esse, avendo ad oggetto il trattamento di dati biometrici, sono assoggettate a un regime particolarmente rigoroso e, in linea generale, vietate salvo specifiche eccezioni. Nella maggior parte dei casi, inoltre, mancherebbe una base giuridica adeguata a giustificare tali trattamenti, poiché il consenso degli interessati non sempre può considerarsi realmente libero in tali ipotesi[28] e le esigenze di sicurezza o di efficienza organizzativa non sono ritenute sufficienti. A ciò si aggiunga il carattere fortemente invasivo della tecnologia, che risulta sproporzionato rispetto alle finalità perseguite e in contrasto con i principi di necessità e minimizzazione dei dati. Infine, il riconoscimento facciale espone gli individui a rischi elevati per i loro diritti e libertà fondamentali, soprattutto quando è utilizzato in contesti di controllo o sorveglianza sistematica[29].

---

[26] Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014, doc. web n. 3556992, Allegato A.

[27] G. CERRINA FERONI, Intelligenza artificiale e ruolo della protezione dei dati personali, su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742, che analiticamente ricorda come «La sovrapposizione deriva, da un lato, dalla definizione estremamente ampia di IA, che comprende persino gli approcci statistici e, dall'altro lato, dal fatto che i cosiddetti sistemi di IA ad alto rischio sono definiti nella bozza per aree in cui per la stragrande maggioranza sono i dati personali ad essere trattati. Si pensi all'identificazione biometrica, all'istruzione, alla sanità, alle prestazioni assistenziali, all'immigrazione, ecc. Solo nel settore delle infrastrutture il Regolamento IA potrebbe avere un'applicazione del tutto autonoma. Negli altri settori vi sarebbe, di fatto, una coregolamentazione e, probabilmente, saranno le normative in materia di protezione dei dati personali a prevalere in quanto competenti per materia. La bozza di Regolamento AI riguarda poi in larga parte oggetti e i principi già enucleati nel GDPR (sebbene l'approccio al rischio diverga perché l'uno responsabilizza il titolare del trattamento ponendo al centro i diritti dell'interessato, l'altro invece introduce un meccanismo di compliance a standard predefiniti dall'alto). Entrambe le leggi si concentrano sulle finalità del trattamento dei dati personali, sull'utilizzo del sistema di IA, sull'approccio by design; entrambi richiedono che gli indirizzi del Regolamento identifichino i rischi per i diritti fondamentali. Tuttavia, la proposta di Regolamento si propone esplicitamente di avere un approccio «umano-centrico» e di plasmare IA che siano affidabili e sicure per gli individui».

[28] Il Garante ha precisato ciò soprattutto con specifico riferimento all'utilizzo di tali tecnologie nell'ambito lavorative. Cfr. *supra* nota n. 18.

[29] In ambito lavorativo, numerosi sono stati i casi sanzionati di datori di lavoro che utilizzassero sistemi di riconoscimento facciale per l'accesso ai luoghi di lavoro e la rilevazione delle presenze dei lavoratori. In tutte tale ipotesi, il Garante ha confermato che l'ordinamento vigente non consente il trattamento dei dati biometrici dei dipendenti, per finalità di rilevazione della presenza in servizio. Per tale ragione, i trattamenti effettuati per tali finalità e non legittimati da alcuna delle condizioni previste dall'art. 9, parag. 2, del GDPR, sono da considerarsi illeciti (ex pluris, provvedimento 6 giugno 2024, doc. web 10029500, provvedimenti del 22 febbraio 2024, doc. web n. 9995785, doc. web 9995701, doc. web 9995680 e doc. web 9995741). Provvedimento del 13 aprile 2023, doc. web n. 9896412 sul nuovo algoritmo di rilevamento dei volti, basato su reti neurali convoluzionali (CNN) che prevede anche una funzione di tracking dell'osservatore. Nel caso specifico si trattava di un sistema di face *detection* che non memorizza permanentemente le caratteristiche facciali del volto individuato. Al contrario dei sistemi di face *recognition,* i sistemi di face *detection* non sono, infatti, finalizzanti a riconoscere determinate persone e non sono connessi all'identificazione e al riconoscimento degli

4. L'impatto sui cittadini: una recente applicazione del riconoscimento facciale nel *Faceboarding*

Le coordinate normative e teoriche sin qui delineate trovano una concreta verifica applicativa nei recenti casi di utilizzo del riconoscimento facciale in ambito aeroportuale, che consentono di misurare l'impatto effettivo delle scelte regolatorie europee sulla vita dei cittadini.

Oggi, il bilanciamento degli interessi effettuato in base al diverso contesto normativo e sociale in cui l'attività di riconoscimento facciale si svolge può comportare effetti pratici molti diversi e, soprattutto, un impatto dirompente sulle condizioni di vita dei cittadini e dei consumatori. Con l'avanzamento tecnologico, che permea ormai con i suoi prodotti sempre più raffinati ed efficaci una vasta gamma di nuovi servizi e permette uno snellimento consistente di procedure burocratiche di identificazione personale (per esempio ai fini di sicurezza), potrebbe risultare più accettabile diminuire le garanzie di tutela della *privacy* in presenza di una maggiore precisione ed efficacia delle misure di controllo nonché di una riduzione notevole dei tempi di accertamento e delle risorse da impiegare.

Una recente applicazione di tali tecnologie all'interno dei confini europei è oggi rappresentata dagli attuali progetti europei di *Smart Borders*, come il Sistema di Ingresso/Uscita (EES) e l'autorizzazione di viaggio ETIAS, che mirano a combinare sicurezza, efficienza e gestione biometrica dei flussi di viaggiatori nell'area Schengen. Questi sistemi permettono di automatizzare e velocizzare i controlli alle frontiere, riducendo la necessità di intervento umano e sfruttando i dati biometrici per garantire al contempo la sicurezza e la regolarità degli spostamenti[30].

interessati. In ogni caso, il sistema utilizzato permette di acquisire informazioni relative all'età, al genere e ad alcuni elementi emotivi dei volti individuati sui diversi fotogrammi […] Sebbene, perciò, il sistema descritto non preveda un trattamento delle immagini del volto dei visitatori, finalizzato al riconoscimento e all'identificazione di tipo biometrico, è innegabile che il funzionamento del sistema sia basato su un'iniziale acquisizione di immagini del volto dei visitatori, successivamente elaborate proprio al fine di individuare, all'interno di esse, i visi.

[30] Il Regolamento (UE) 2025/1534, adottato il 18 luglio 2025 (il cui contenuto era stato in parte anticipato dal Reg. (UE) 2017/2225 con l'introduzione di un sistema di controlli automatizzati assicurato dall'interoperabilità di banche dati nazionali), disciplina l'avvio graduale del sistema Entry/Exit System (EES), previsto dalla normativa dell'UE per la gestione digitale delle frontiere esterne dello spazio Schengen tramite l'iniziativa dei c.d. Smart Borders ("Frontiere Intelligenti"). Questo nuovo sistema è composto dal Sistema di Ingresso/Uscita (EES), lanciato ufficialmente il 12 ottobre 2025. L'EES sostituisce i timbri manuali sui passaporti per i cittadini non UE che entrano o escono dagli Stati Schengen, registra automaticamente dati biometrici e di viaggio (come le impronte digitali, scansione del volto, date e punti di ingresso/uscita), migliora la sicurezza delle frontiere, serve a controllare meglio gli ingressi e le uscite, combattere le frodi d'identità e tracciare eventuali soggiorni oltre la durata consentita. Una volta implementato, non verranno più apposti timbri manuali sui passaporti per i viaggiatori extra-UE. Per definizione di "smart borders" si veda J. P. BURGESS, D. KLOZA (eds.), *Border Control and New Technologies. Addressing Integrated Impact Assessment*, ASP, 2021, che parla di «sistemi automatizzati per accelerare e facilitare la procedura di controllo alle frontiere della maggior parte dei viaggiatori, e per ostacolare e fermare quegli immigrati che rappresentano una minaccia per la sicurezza dell'UE attraverso il loro status di immigrati irregolari, criminali o terroristi». Non mancano, tuttavia, i rischi di politicizzazione di tali dispositivi, nonché i rischi di discriminazione e stigmatizzazione. Sul punto, S. PENASA, *Smart borders o invisibile walls? L'utilizzo di sistemi "intelligenti" al confine tra politiche migratorie e garanzie per gli stranieri,* in *ADiM Blog*, Analisi & Opinioni, dicembre 2022. Le prime criticità operative del sistema hanno già sollevato alcune critiche e creato malfunzionamenti.

Tuttavia, come già visto, l'uso dei dati biometrici e in particolare della tecnologia di riconoscimento facciale continuano a essere considerati, almeno nell'ordinamento europeo, fonti di importanti rischi per i diritti e le libertà degli interessati. Questo approccio determina un significativo rallentamento nel processo di accettazione di tali sistemi, ponendo in ombra i vantaggi e le opportunità che essi possono offrire.

Le conseguenze pratiche del disallineamento dei diversi approcci operativi e legislativi sull'utilizzo dei dati biometrici nelle tecnologie di riconoscimento facciale nelle varie prospettive mondiali potrebbero plasticamente rappresentarsi, in modo molto semplice e intuitivo, confrontando un viaggio aereo da parte dello stesso passeggero tra un paese europeo che applica il GDPR e un Paese (asiatico?) molto più propenso all'applicazione degli strumenti di IA di *Faceboarding*. Le procedure di check-in e di imbarco condotte con strumenti di riconoscimento facciale supportati da IA non comportano più l'esame di documentazione cartacea o digitale (documenti di riconoscimento, pagamenti, etc.) e si svolgono con un semplice passaggio fisico da un varco presso cui si trova uno schermo che identifica il volto e lo associa in tempo reale alle banche dati dei servizi (pubblici e privati) che devono essere controllate affinché si autorizzi la legittima e sicura presenza su quel volo aereo di quel determinato soggetto.

I confronti effettuati in tempo reale dall'IA impiegata in questi controlli non sono neanche lontanamente paragonabili a quelli che potrebbe esperire un addetto umano al varco dell'imbarco o al check-in dell'aeroporto. Ecco perché il riferimento che il GDPR fa all'utilizzo di 'mezzi meno invasivi', come alternativa da preferire all'utilizzo di sistemi di riconoscimento facciale, oggi suona forse piuttosto stucchevole. Qui la scelta è tra uno strumento (l'IA applicata al riconoscimento dei dati biometrici) che riesce a sondare – ma con un 'addestramento' massiccio - profondità informative prima irraggiungibili con gli strumenti tradizionali e con il mero controllo umano e una prassi tradizionale (o minimamente digitalizzata) che, per cercare di bilanciare gli interessi in gioco, finisce per legittimare un procedimento burocratico che diventa, alla luce degli sviluppi tecnologici in atto, inevitabilmente percepito come obsoleto, molto più costoso in termini di risorse impiegate e di tempo dedicato e senz'altro poco utile a perfezionare la resa dinamica dell'IA dedicata. Peraltro, le potenzialità (futuribili) di un sistema di interconnessione internazionale delle banche dati detenute dai vari Governi potrebbero portare ad una capillarità nella gestione delle informazioni che, probabilmente, aumenterebbe esponenzialmente l'efficacia dei controlli sugli spostamenti di soggetti pericolosi a tutto vantaggio della sicurezza e della tranquillità della generalità dell'utenza e degli equipaggi.

Sul punto si veda L. BERBERI, *Voli, aeroporti europei in crisi per i nuovi controlli sui passeggeri stranieri: «Attese di 3 ore, Bruxelles intervenga»*, in *Corrieredellasera.it* del 18 dicembre 2025.

Il tema è stato di recente oggetto di attenzione delle cronache (è il noto caso del *Faceboarding* dell'aeroporto di Milano Linate nei confronti del quale l'Autorità italiana ha emesso un provvedimento inibitorio[31]) e il Garante della Privacy italiano si è trovato nella necessità di smentire di aver bloccato il ricorso al riconoscimento facciale negli aeroporti italiani, precisando che il provvedimento adottato nei confronti della società gestore dello scalo milanese (S.E.A) è stato motivato da altre ragioni[32]. Infatti, il caso del *Faceboarding* presso l'aeroporto di Milano Linate assume un valore emblematico, in quanto rappresenta una vera e propria cartina di tornasole delle tensioni esistenti tra esigenze di efficienza operativa, innovazione tecnologica e tutela dei diritti fondamentali.

Il Garante della Privacy italiano, nel negare la legittimità dell'installazione e dell'utilizzo di un sistema di riconoscimento facciale tramite *Faceboarding* da parte della società S.E.A ha tenuto conto del parere n. 11/2024 adottato dal Comitato europeo per la protezione dei dati il 24.05.2024 denominato "*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)*".

Tale atto dell'autorità europea esamina la legittimità, rispetto alle disposizioni di cui agli artt. 5, paragrafo 1, lettere e) e f) (principio di limitazione della conservazione e principi di integrità e riservatezza), 25 (principi di privacy by design e privacy by default) e 32 (sicurezza del trattamento) del GDPR del trattamento dei dati biometrici dei passeggeri effettuato tramite sistemi di riconoscimento facciale presso le aree aeroportuali al fine di facilitare le operazioni di accesso e di controllo del flusso. In questa occasione, il Comitato europeo ha mostrato una piccola – ma significativa – apertura verso tali modelli[33], dichiarando la conformità di tali trattamenti con gli articoli 5, 25 e 32 GDPR summenzionati nel caso in cui l'architettura preveda la conservazione del modello biometrico in capo al passeggero (ad es. localmente su un suo dispositivo) e, invece, escludendola nel caso in cui si preveda una conservazione

[31] *Milano Linate diventa un aeroporto full biometric. Col Faceboarding l'imbarco è possibile mostrando solo il volto*. È con questo titolo che la società S.E.A. annuncia nel proprio sito l'avvio del *Faceboarding*: il nuovo servizio che consente ai passeggeri di Milano Linate di accedere ai controlli di sicurezza e di effettuare le procedure di imbarco attraverso un innovativo sistema di riconoscimento facciale. Nel *footer* del sito è dedicato ampio spazio al trattamento dei dati personali ove si specifica che "*La privacy dei viaggiatori è una delle priorità di SEA Milan Airports. Tutti i passeggeri che aderiranno al servizio Faceboarding forniscono i consensi per autorizzare il sistema a scansionare i dati presenti sul documento di identità, i dati della carta d'imbarco ed il volto. I dati vengono trattati solo ai fini di adesione al servizio. In particolare, le immagini del volto non sono conservate, ma vengono utilizzate esclusivamente per creare un modello biometrico necessario per l'accesso ai controlli di sicurezza e, eventualmente, ai gate di imbarco*".

[32] Garante Privacy '*Nessun divieto generale all'utilizzo del riconoscimento facciale in aeroporto*' (comunicato stampa del 18.09.2025)

[33] L'atteggiamento assunto dall'EDPB risulta essere particolarmente prudente e ciò lo si coglie dalle precisazioni fatte circa l'ambito di applicazione del parere nei seguenti termini "4) *A tale riguardo il presente parere non include un'analisi completa ed esaustiva della conformità al GDPR da parte del relativo titolare o dei relativi titolari del trattamento in ciascun caso, nonché del loro responsabile o dei loro responsabili del trattamento, se del caso. […] Il presente parere non pregiudica pertanto una valutazione relativa ad altre disposizioni del GDPR per quanto riguarda l'uso di tecnologie di riconoscimento facciale, anche nel settore specifico oggetto della richiesta o un'analisi giuridica e tecnica caso per caso basata sulle circostanze e sul trattamento specifici previsti da un titolare del trattamento; 5) il presente parere non esamina il trattamento dei dati personali dei minori e non pregiudica gli eventuali requisiti specifici applicabili a tale riguardo; […]7) qualsiasi conclusione contenuta nel presente parere non pregiudica gli ulteriori sviluppi tecnologici;* (parag. 13.4 e ss.). Il parere è consultabile nel sito dell'EDPB.

centralizzata riconducibile all'autorità aeroportuale o, peggio ancora, in capo alla compagnia aerea tramite l'uso di servizi in cloud. Infatti, l'elemento di *discrimen* per riconoscere la conformità di tali modelli col GDPR sembra proprio essere il fatto che si mantenga in capo all'interessato il potere sui propri dati ed essa sia invece da escludere ogni qual volta il trattamento esca fuori dalla sua sfera di controllo e sia affidata al Titolare (es. ente aeroportuale) o a Responsabili esterni (es. fornitore delle piattaforme *cloud* utilizzate dal gestore aeroportuale)[34].

In questo contesto è dunque da inserirsi il provvedimento del Garante privacy italiano emesso nei confronti del gestore aeroportuale dello scalo milanese. Infatti, Il sistema proposto da S.E.A. si sarebbe basato sulla conservazione centralizzata dei modelli biometrici dei passeggeri presso lo stesso gestore aeroportuale, senza che fosse prevista la cifratura di tali modelli tramite chiave in possesso dei passeggeri. Si tratterebbe di un modello, dunque, basato su una gestione centralizzata del trattamento (dall'acquisizione dei dati, compresa la conservazione, e sino alla loro cancellazione) interamente in capo al gestore aeroportuale e senza che sia assicurato il mantenimento di un effettivo potere di controllo dell'interessato sui propri dati (ad es. tramite il possesso in capo esclusivamente a quest'ultimo della chiave di cifratura). Di conseguenza, tale trattamento, seppur basato sul consenso esplicito dell'interessato (acquisito per il tramite dei chioschi situati nelle immediate vicinanze dei varchi o mediante l'App dedicata[35]), non consentirebbe un controllo attivo da parte dell'interessato sui propri dati biometrici, che rimangono nell'esclusiva disponibilità del gestore aeroportuale.

Da tali elementi il Garante italiano, dunque, ha dedotto la riconducibilità della soluzione di *Faceboarding* a uno degli scenari descritti nel Parere dell'EDPB n. 11/2024 (scenario n. 3) ritenuto non conforme all'art. 5, paragrafo 1, lett. f), e agli articoli 25 e 32 GDPR.

Altro punto cruciale rilevato dall'Autorità Garante, come ulteriore elemento per escludere la conformità del modello al GDPR, ha riguardato l'informativa resa agli interessati ai sensi dell'art. 13 del Regolamento,

[34] Più precisamente, il trattamento dei dati personali con sistemi di riconoscimento facciale, secondo il parere, è consentito con esclusivo riferimento alle ipotesi denominate "Scenario 1 - conservazione del modello biometrico registrato solo nelle mani della persona ai fini dell'autenticazione" (v. sez. 3.2.1 dell'Opinion n. 11/2024) e "Scenario 2 - conservazione centralizzata del modello biometrico registrato in forma cifrata all'interno dell'aeroporto e con una chiave segreta nota esclusivamente ai passeggeri ai fini dell'autenticazione" (v. sez. 3.2.2 dell'Opinion n. 11/2024). Non sono invece conformi al GDPR i trattamenti effettuati nel contesto degli altri due scenari contemplati nel parere, denominati rispettivamente "Scenario 3.1- conservazione centralizzata dei modelli biometrici in una banca dati all'interno dell'aeroporto, sotto il controllo del gestore aeroportuale" (v. sez. 3.2.3.1 dell'Opinion n. 11/2024) e "Scenario 3.2 - conservazione centralizzata dei modelli biometrici in un cloud sotto il controllo della compagnia aerea" (v. sez. 3.2.3.2 dell'Opinion n. 11/2024).

[35] Rispetto all'App è stato verificato che, all'interno delle "*Digital Travel Credential*" presenti nell'App, erano memorizzate soltanto le informazioni presenti nel documento d'identità e "l'immagine del volto dell'interessato acquisita tramite selfie", mentre "il *template* biometrico resta conservato esclusivamente nel sistema centralizzato della Società". Le misure di sicurezza delle "Digital Travel Credential" non sono state ritenute idonee a consentire di assicurare un controllo attivo, da parte dell'interessato, sui propri dati biometrici, che rimanevano, invece, nell'esclusiva disponibilità del gestore aeroportuale.

la quale precisava che il modello biometrico (e quindi il complesso dei dati biometrici che consentivano l'identificazione dell'interessato) rimanesse conservato esclusivamente nel dispositivo del passeggero, cosa che invece non avveniva in quanto dall'istruttoria dell'autorità era emerso che tali dati venissero conservati nel sistema centralizzato di S.E.A.

Ma, rilievo ancor più pregnante sembra essere quello in base al quale i varchi dedicati al *Faceboarding* fossero di natura ibrida, in quanto utilizzabili anche per il transito di passeggeri che non avessero aderito al già menzionato sistema di identificazione e autenticazione. Rispetto a tali passeggeri il sistema era in grado di generare un template biometrico a seguito dell'acquisizione dell'immagine del passeggero transitante. Ciò, evidentemente, ha destato significativi dubbi di legittimità del trattamento (mancando il consenso dell'interessato) e di trasparenza.

Il caso di Linate rappresenta senza dubbio uno tra i momenti più significativi di riflessione sull'utilizzo dei sistemi di riconoscimento facciale in Italia. Tuttavia, le violazioni riscontrate — in particolare quelle riguardanti le inesattezze nell'informativa ai sensi dell'art. 13 del Regolamento e l'uso di dati biometrici anche di passeggeri non aderenti al servizio — hanno portato a un provvedimento inibitorio *necessitato*. Ciò rende ancora più difficile comprendere quale sia la posizione dell'Autorità Garante sull'impiego di tali sistemi e se, al netto dei motivi di inibizione, il provvedimento rappresenti comunque una qualche apertura rispetto agli orientamenti precedenti sul tema del riconoscimento facciale[36].

All'indomani del provvedimento citato era dunque legittimo chiedersi se l'inibitoria sarebbe stata comunque emessa anche nel caso in cui il sistema fosse stato classificabile come uno degli scenari ritenuti dall'EDPB conformi ai principi privacy (come ad es. lo Scenario 1 o 2). Sembra che però tale perplessità abbia aleggiato tra gli uffici di Piazza Venezia al punto che, solo qualche giorno dopo l'emissione del provvedimento nei confronti della S.E.A., è stato diffuso un comunicato stampa tramite il quale l'Autorità ha voluto chiarire che in Italia non vi è alcun divieto assoluto e generale circa l'utilizzo di tecnologie di riconoscimento facciale in aeroporto, ma occorre che esse siano sviluppate secondo soluzioni tecnologiche "*diverse da quella adottata da SEA, idonee a bilanciare le esigenze di semplificazione nelle operazioni di imbarco con quelle di protezione dei dati personali nel rispetto della vigente disciplina europea, con particolare riferimento al trattamento dei dati biometrici. Tali soluzioni sono quelle specificatamente indicate nel citato parere dal Comitato*[37]".

In altre parole, sembra che l'Autorità abbia inteso aprire uno spiraglio nei confronti di tali sistemi, a patto che essi siano strutturati in modo conforme a quanto stabilito dall'EDPB.

[36] Basti pensare alla posizione assunta dall'Autorità con riguardo all'utilizzo di sistemi di riconoscimento facciale nel contesto lavorativo, ove nemmeno il consenso rappresenterebbe un'idonea base giuridica (cfr. nota 18 *supra*) e il parere negativo espresso dall'Autorità emesso con riguardo all'utilizzo del sistema Sari Real Time da parte del Ministero dell'Interno, rispetto al quale ancora oggi risulta bloccata la sperimentazione alla luce dei dubbi sulla sua conformità alla normativa privacy.

[37] Il comunicato stampa del Garante è consultabile nel sito dell'autorità.

Al netto di queste singole vicende, la sensazione tra gli operatori è quella di un atteggiamento estremamente prudente dell'Autorità italiana, in attesa di una chiara presa di posizione da parte del legislatore. Del resto, lo stesso legislatore italiano – anche su spinta di quello comunitario - ha assunto un atteggiamento analogo rispetto a questo tipo di sperimentazioni, che per certi versi sembra andare in direzione opposta rispetto alla tendenza rinvenibile in altri ordinamenti (extra SEE). Infatti, il decreto-legge n. 51/2023 ha previsto l'estensione al 31 dicembre 2025[38] del divieto di installazione di nuovi impianti di videosorveglianza dotati di riconoscimento facciale in luoghi pubblici. Tale posizione pare assunta per consentire di monitorare l'evoluzione delle normative europee, in particolare l'AI Act.

A tali considerazioni si aggiunga il fatto che la Legge 132/2025 (c.d. DDL IA) non contiene alcuna disposizione riferibile ai sistemi di riconoscimento facciale. È forse questa una voluta dimenticanza, in attesa che il contesto – normativo in primis – sia più chiaro?

In sintesi, il caso di Milano Linate evidenzia come l'Italia stia adottando un approccio prudente e cautelativo verso il riconoscimento facciale in aeroporto, bilanciando le opportunità offerte dall'innovazione tecnologica con la necessità di tutelare i diritti fondamentali, in attesa di un quadro normativo europeo e nazionale più definito.

5. Conclusioni

L'analisi svolta ha mostrato come le tecnologie di riconoscimento facciale rappresentino oggi uno dei terreni più sensibili e controversi dell'evoluzione dell'intelligenza artificiale, collocandosi all'intersezione tra innovazione tecnologica, sicurezza, interessi economici e tutela dei diritti fondamentali. Infatti, la sua evoluzione tecnologica, sostenuta da tecniche avanzate di apprendimento automatico e dall'uso massivo di dati, ha ampliato in modo significativo le potenzialità applicative, ma anche i rischi giuridici ed etici.

Il confronto tra i diversi approcci socio-politici all'uso del riconoscimento facciale ha evidenziato che, a seconda dei diversi approcci adottati nei vari sistemi socio-politici, il c.d. 'addestramento' dell'intelligenza artificiale sotteso alla gestione dei sistemi di FRT sarà molto diverso: un approccio con molte più limitazioni nella gestione dei dati biometrici di FRT può comportare una minore resa dell'IA utilizzata per questo scopo, con il rischio che la forbice di efficacia tra i vari sistemi di IA si allarghi a dismisura nel tempo.

L'impatto concreto di tali scelte regolatorie emerge con particolare chiarezza nell'analisi delle applicazioni pratiche, come dimostra il caso del *Faceboarding* in ambito aeroportuale. La vicenda dello scalo di Milano Linate e il relativo intervento del Garante per la protezione dei dati personali evidenziano come la

[38] L'art. 8 ter del decreto-legge citato ha modificato l'art. 9, co. 9, del decreto-legge 139/2021, così spostando la scadenza originariamente prevista dal 31 dicembre 2023 al 31 dicembre 2025.

legittimità di questi sistemi non dipenda soltanto dalla finalità perseguita o dal consenso formale degli interessati, ma soprattutto dall'architettura tecnologica adottata e dal mantenimento di un effettivo controllo dei dati biometrici in capo agli individui. In questo senso, il parere dell'EDPB n. 11/2024 segna un passaggio significativo, aprendo alla possibilità di modelli tecnici compatibili con il GDPR, ma al contempo fissando confini stringenti a tutela dei diritti.

Nel complesso, emerge un quadro caratterizzato da una tensione strutturale tra esigenze di efficienza, sicurezza e innovazione, da un lato, e protezione dei diritti fondamentali, dall'altro. L'approccio prudente adottato dall'Unione europea e, in particolare, dall'ordinamento italiano, appare coerente con la tradizione giuridica di tutela della persona, ma solleva interrogativi rilevanti sul piano della competitività tecnologica e del rischio di un progressivo disallineamento rispetto ad altri contesti extraeuropei.

La sfida futura sarà individuare un equilibrio tra tutela dei diritti fondamentali e sviluppo tecnologico, evitando sia derive di sorveglianza incompatibili con i valori democratici sia un eccesso di cautela che possa ostacolare l'innovazione. In questo senso, il riconoscimento facciale rappresenta un banco di prova per la capacità dell'ordinamento europeo di governare l'intelligenza artificiale in modo coerente con la propria identità valoriale.

I dubbi sono molti e i quesiti aperti ancora di più. Ciò che è certo è che viviamo in un contesto con protagonisti che corrono a velocità diverse e l'approccio prudente e più riflessivo dell'Italia evidenzia una diversa velocità di progresso.