

UNIVERSITÀ DEGLI STUDI DI GENOVA

**SCUOLA DI SCIENZE SOCIALI
DIPARTIMENTO DI GIURISPRUDENZA**



Corso di Laurea magistrale in Giurisprudenza

Dissertazione di Laurea in Diritti di libertà e diritti sociali

**I SISTEMI DI RICONOSCIMENTO FACCIALE E IL
POSSIBILE CONTRASTO CON I DIRITTI
FONDAMENTALI**

LA RELATRICE:

Chiar.^{ma} Prof.ssa Francesca Bailo

LA CANDIDATA:

Martina Durante

Anno Accademico 2025 – 2026

*Alla mia famiglia, che ha custodito il mio cammino
come un porto accoglie chi rientra dal mare.*

*A me stessa, per aver continuato a navigare anche
nei giorni più difficili.*

SOMMARIO

Introduzione.....	1
Capitolo 1- Il riconoscimento facciale: tecnologia, sorveglianza e diritti fondamentali.....	3
1. Dalle tecnologie di videosorveglianza al riconoscimento facciale	3
2. I sistemi di riconoscimento facciale e i dati biometrici: struttura e funzionamento.....	7
3. La ridefinizione dei diritti fondamentali nell'era della sorveglianza biometrica	11
3.1 L'incidenza del riconoscimento facciale sui diritti individuali	11
3.2 L'incidenza del riconoscimento facciale sui diritti partecipativi e sulla dimensione democratica.....	18
Capitolo 2 - Il quadro normativo europeo e italiano	25
1. La disciplina europea del riconoscimento facciale tra protezione dei dati personali e regolazione dell'intelligenza artificiale	25
1.1 Tutela dei dati biometrici e principi del trattamento alla luce del GDPR	25
1.2 Requisiti e obblighi per i sistemi di intelligenza artificiale alla luce dell' <i>AI Act</i>	31
2. Le autorità di controllo nel sistema europeo di protezione dei dati	34
3. Italia: dal Codice <i>privacy</i> alla legge 132/2025.....	37
4. Il Garante per la protezione dei dati personali e i sistemi di riconoscimento facciale – un'analisi per casi.....	47
4.1 Il caso SARI – tra l'investigazione e l'identificazione biometrica in tempo reale.....	47
4.1.1 I più recenti sviluppi dell'attuazione nazionale dell' <i>AI Act</i> in materia di identificazione biometrica.....	53
4.2 Il caso <i>Clearview AI</i>	58
4.3 Le sperimentazioni del riconoscimento facciale negli aeroporti – <i>faceboarding</i>	60
4.4 Il riconoscimento facciale e i rapporti tra privati.....	62
4.5 Tra prudenza e principi, l'approccio del Garante <i>privacy</i> al riconoscimento facciale	65
Capitolo 3 - Modelli internazionali di regolazione del riconoscimento facciale.....	68
1. Il modello di sorveglianza totale cinese	69
2. Il sistema <i>Aadhaar</i> indiano: identità biometrica e accesso ai servizi.....	77
3. Giamaica e Kenya: identità digitale nazionale e biometria amministrativa	82
4. Il modello “innovativo” americano.....	87
5. Il modello russo e il caso Glukhin c. Russia della Corte EDU	92
Conclusioni	97
Bibliografia e sitografia	103
Giurisprudenza.....	110
Normativa	112
Soft law e documenti istituzionali.....	113

Introduzione

Nel 1996 John Perry Barlow immaginava il cyberspazio come uno spazio sottratto alla sovranità degli Stati e affidato a forme di autoregolazione proprie della comunità digitale¹. A distanza di quasi trent'anni, tale rappresentazione appare però profondamente ridimensionata. Lo sviluppo delle tecnologie biometriche e, in particolare, dei sistemi di riconoscimento facciale ha mostrato come l'ambiente digitale non sia affatto neutro, ma costituisca uno spazio nel quale si concentrano nuove forme di potere capaci di incidere direttamente sulla sfera giuridica delle persone. In questo contesto, il diritto non si pone necessariamente come ostacolo all'innovazione, ma come strumento di orientamento e contenimento dei suoi possibili effetti lesivi. In tale prospettiva, la protezione dei dati personali assume il significato di presidio dell'autodeterminazione individuale nella società dell'informazione², sino a essere riconosciuta, nell'esperienza europea, come diritto fondamentale autonomo³.

In questa cornice si colloca il tema del presente lavoro, dedicato all'analisi dei sistemi di riconoscimento facciale e del loro possibile contrasto con la tutela dei diritti fondamentali. Tali tecnologie rappresentano una delle applicazioni più controverse dell'intelligenza artificiale applicata all'identificazione personale, in quanto consentono l'identificazione automatica degli individui attraverso il trattamento di dati biometrici, incidendo su una pluralità di diritti fondamentali, tra cui il diritto alla riservatezza, il diritto alla protezione dei dati personali, il principio di eguaglianza e il divieto di discriminazione.

La possibilità di identificare automaticamente le persone nello spazio pubblico, anche attraverso infrastrutture digitali, solleva interrogativi particolarmente rilevanti circa i limiti del potere tecnologico e il ruolo del diritto nel governarne gli sviluppi. L'impiego di tali tecnologie, infatti, può tradursi in forme di monitoraggio diffuso idonee a incidere sull'esercizio delle libertà fondamentali.

¹ V. J. P. BARLOW, *A Declaration of the Independence of Cyberspace* in EFF (www.eff.org), 8 febbraio 1996

² Cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 46 ss.; cfr. S. RODOTÀ, *Il diritto di avere diritti*, editori Laterza, Roma, 2012, pag. 270 s.

³ V. art. 8 CDFUE; cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, 2019, pag. 10

Alla luce di tali premesse, la presente tesi si propone di analizzare se e in che misura l'attuale quadro normativo europeo e nazionale sia idoneo a garantire un adeguato bilanciamento tra innovazione tecnologica e tutela dei diritti fondamentali. L'obiettivo non è soltanto quello di ricostruire il panorama normativo esistente, ma anche di verificare se l'attuale sistema regolatorio sia effettivamente in grado di contenere le potenzialità invasive delle tecnologie di riconoscimento facciale o se permangano lacune e/o criticità nella disciplina vigente.

A tal fine, il lavoro si articola in tre parti principali. Nel primo capitolo vengono analizzate le caratteristiche tecnologiche dei sistemi di riconoscimento facciale e i principali diritti fondamentali potenzialmente coinvolti dal loro utilizzo. Il secondo capitolo è dedicato all'esame del quadro normativo europeo e nazionale, con particolare attenzione ai principi e obblighi derivanti dal GDPR e dall'AI Act, oltreché al ruolo svolto dalle autorità di protezione dei dati personali, il cui approccio viene ricostruito tramite l'analisi dei casi SARI e Clearview AI, delle esperienze sul faceboarding e dell'impiego delle tecnologie di riconoscimento facciale nei rapporti tra privati. Il terzo capitolo propone, infine, un'analisi comparata di alcune esperienze internazionali, al fine di evidenziare le diverse modalità con cui gli ordinamenti giuridici affrontano il rapporto tra sicurezza, innovazione tecnologica e tutela dei diritti.

Il riconoscimento facciale costituisce uno dei terreni sui quali si misura oggi la capacità del diritto di confrontarsi con l'innovazione tecnologica senza sacrificare la tutela della persona. In tale prospettiva, l'analisi del quadro normativo vigente consente di verificare se gli strumenti giuridici attualmente disponibili siano effettivamente adeguati rispetto ai rischi che queste tecnologie possono comportare.

Capitolo 1

Il riconoscimento facciale: tecnologia, sorveglianza e diritti fondamentali

SOMMARIO: 1. Dalle tecnologie di videosorveglianza al riconoscimento facciale. – 2. I sistemi di riconoscimento facciale e i dati biometrici: struttura e funzionamento. – 3. La ridefinizione dei diritti fondamentali nell'era della sorveglianza biometrica. – 3.1. L'incidenza del riconoscimento facciale sui diritti individuali. – 3.2. L'incidenza del riconoscimento facciale sui diritti partecipativi e sulla dimensione democratica.

L'evoluzione tecnologica ha profondamente trasformato le modalità attraverso cui gli individui possono essere identificati nello spazio pubblico. Tra le innovazioni più significative e controverse si collocano i sistemi di riconoscimento facciale, che uniscono capacità avanzate di elaborazione algoritmica alla possibilità di identificare automaticamente le persone attraverso il trattamento dei dati biometrici.

Prima di passare all'analisi del quadro normativo e istituzionale che disciplina le suddette tecnologie, è opportuno ricostruirne l'evoluzione tecnologica, il funzionamento tecnico e le principali implicazioni in termini di diritti fondamentali.

1. Dalle tecnologie di videosorveglianza al riconoscimento facciale

La diffusione dei sistemi di riconoscimento facciale è il risultato di un processo evolutivo che ha interessato, nel corso degli ultimi decenni, le tecnologie di videosorveglianza⁴.

Le prime forme di videosorveglianza risalgono agli anni Sessanta quando le telecamere analogiche furono installate in contesti caratterizzati da peculiari esigenze di sicurezza come le banche, le strutture militari o le infrastrutture strategiche. Questi sistemi si basavano su circuiti chiusi che permettevano la visualizzazione delle

⁴ Cfr. C. NORRIS, M. MCCAHERN, D. WOOD, *Editorial. The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space*, in *Surveillance & Society*, 2004, pag. 110 ss.

immagini in tempo reale su monitor dedicati, ma non disponevano ancora di capacità di analisi automatica o di archiviazione avanzata dei dati⁵.

A partire dagli anni Settanta l'utilizzo delle telecamere iniziò a diffondersi anche negli spazi urbani, soprattutto nelle aree ad alta densità demografica, contribuendo alla progressiva affermazione di forme di sorveglianza costante nelle grandi città. I progressi tecnologici del decennio seguente, poi, portarono all'integrazione dei sistemi di videosorveglianza con dispositivi in grado di rilevare il movimento, permettendo alle telecamere di attivarsi in automatico in presenza di determinate azioni o anomalie comportamentali. In questo periodo i sistemi analogici furono progressivamente sostituiti da registratori video digitali – c.d. DVR – che agevolarono la conservazione e la gestione delle registrazioni video⁶.

I primi studi sul riconoscimento automatico dei volti risalgono in realtà agli anni Sessanta del Novecento, quando alcuni ricercatori statunitensi iniziarono a sviluppare modelli sperimentali di analisi delle caratteristiche facciali tramite elaborazione informatica delle immagini. In particolare, i lavori condotti da Woodrow W. Bledsoe presso il Panoramic Research Institute rappresentano uno dei primi tentativi di costruire sistemi in grado di identificare un volto umano attraverso l'analisi di specifici punti del viso⁷. Tali esperimenti però erano ancora fortemente limitati dalle capacità di calcolo disponibili all'epoca, pertanto restarono confinati nell'ambito della ricerca accademica⁸.

Il riconoscimento facciale iniziò ad emergere negli anni Novanta come possibile applicazione dei sistemi di videosorveglianza tradizionali. In questa fase iniziarono a essere sviluppati i primi algoritmi volti a individuare e analizzare alcune caratteristiche

⁵ Cfr. C. NORRIS, M. MCCAILL, D. WOOD, *Editorial. The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space*, in *Surveillance & Society*, 2004, pag. 119

⁶ Cfr. C. NORRIS, M. MCCAILL, D. WOOD, *Editorial. The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space*, in *Surveillance & Society*, 2004, pag. 119 s.; Cfr. W. HU, T. TAN, L. WANG, S. MAYBANK, *A survey on visual surveillance of object motion and behaviors*, in *IEEE transactions on systems, man, and cybernetics*, vol. 34, n. 3, agosto 2004, pag. 335 ss.

⁷ Cfr. *Facial Recognition Technology: current capabilities, prospects and governance*, in National Academies (www.nationalacademies.org), pag. 34 ss.; cfr. I.D. RAJI, G. FRIED, *About face: a survey of facial recognition evaluation*, in Arxiv (www.arxiv.org), Period I: Research Findings (1964-1995), 2021

⁸ Cfr. I.D. RAJI, G. FRIED, *About face: a survey of facial recognition evaluation*, in Arxiv (www.arxiv.org), Period I: Early Research Findings (1964-1995), 2021

del volto umano al fine di consentire l'identificazione automatica degli individui⁹. Sebbene si trattasse ancora di tecnologie sperimentali, verso metà anni Novanta furono realizzati i primi sistemi commerciali di riconoscimento facciale, utilizzati soprattutto in contesti di sicurezza e di controllo delle identità dei passeggeri. Questi sistemi però, si caratterizzavano per costi molto elevati e una accuratezza limitata e ciò ne limitava la diffusione¹⁰.

Nel corso degli anni Duemila la videosorveglianza divenne sempre più automatizzata grazie all'integrazione di software in grado di analizzare i video per rilevare movimenti sospetti o anomalie comportamentali. Parallelamente, i progressi nel campo dell'intelligenza artificiale e delle reti neurali permisero una maggiore accuratezza dei sistemi di riconoscimento facciale e questi iniziarono a essere usati anche nei contesti urbani¹¹. In alcune città queste tecnologie iniziarono a essere sperimentate dalle forze dell'ordine come strumenti di supporto alle attività investigative e di monitoraggio degli spazi pubblici. Tali sistemi sebbene fossero ancora molto costosi e poco diffusi, segnarono l'inizio dell'impiego di tali tecnologie a scopi di sicurezza¹².

La vera svolta per la videosorveglianza e il riconoscimento facciale avvenne circa nel 2010, quando l'accuratezza degli algoritmi migliorò in modo esponenziale grazie allo sviluppo delle tecniche di apprendimento automatico¹³. Contestualmente, anche grandi piattaforme digitali iniziarono a usarle: si pensi ad esempio all'introduzione da parte di Facebook di sistemi di riconoscimento automatico dei volti per i tag delle fotografie

⁹ Cfr. A.K. JAIN, A.ROSS, S. PRABHAKAR, *An Introduction to Biometric Recognition*, in IEEE transaction on circuits and system for video technology, vol. 14, n. 1, gennaio 2004 pag. 6; v. J. PHILIPS, P.J. RAUSS, S.Z. DER, FERET (Face Recognition Technology), *Recognition Algorithm Development and Test results*, in NIST (www.nist.org), ottobre 1996, pag. 9 s.

¹⁰ Cfr. J. PHILIPS, P.J. RAUSS, S.Z. DER, FERET (Face Recognition Technology), *Recognition Algorithm Development and Test results*, in NIST (www.nist.org), ottobre 1996, pag. 45; cfr. I.D. RAJI, G. FRIED, *About face: a survey of facial recognition evaluation*, 2021, pag. 2; cfr. P. J. PHILLIPS, P. GROTH, R.J. MICHEALS, D.M. BLACKBURN, E. TABASSI, M. BONE, *Face Recognition Vendor Test 2002: Evaluation Report*, in NIST, 2003, pag. 4 ss.

¹¹ Cfr. *Facial Recognition Technology: current capabilities, prospects and governance*, in National Academies (www.nationalacademies.org), pag. 36 s.

¹² Cfr. J. PHILIPS, P.J. RAUSS, S.Z. DER, FERET (Face Recognition Technology), *Recognition Algorithm Development and Test results*, in NIST (www.nist.org), ottobre 1996, pag. 9

¹³ Cfr. *Facial Recognition Technology: current capabilities, future prospects and governance*, in National Academies (www.nationalacademies.org), pag. 31

postate¹⁴. Al contempo le telecamere di sorveglianza, che ora erano integrate con software di analisi automatica delle immagini, sono diventate sempre più comuni nelle città, e talvolta utilizzano l'analisi in tempo reale per identificare facce e comportamenti sospetti¹⁵: si pensi a paesi come la Cina che avevano costruito massicci sistemi di sorveglianza dotati di riconoscimento facciale negli spazi pubblici¹⁶.

Sebbene oggi tali tecnologie siano diffuse in una molteplicità di settori – quali la sicurezza informatica, i sistemi di pagamento elettronico e i controlli di accesso – la loro nascita è strettamente legata alle esigenze di identificazione proprie della pubblica sicurezza. L'identificazione rappresenta, infatti, una procedura fondamentale attraverso la quale le autorità accertano l'identità di un individuo e ne attribuiscono le generalità. Questa esigenza non è nuova nella storia istituzionale, ma si è evoluta nel tempo parallelamente allo sviluppo delle tecnologie disponibili.

Uno dei primi tentativi sistematici di organizzare le procedure di identificazione criminale risale all'opera di Eugène Vidocq, fondatore della Brigade de la Sûreté – ramo della polizia parigina¹⁷. A inizio Ottocento Vidocq contribuì alla creazione di archivi criminali nei quali venivano raccolte informazioni sui soggetti sospettati o condannati per reati, includendo descrizioni dei tratti fisici, cicatrici o segni particolari.

Sul finire dell'Ottocento il sistema fu ulteriormente sviluppato da Alphonse Bertillon¹⁸ che introdusse un metodo di identificazione fondato sulla misurazione sistematica di specifiche caratteristiche fisiche degli individui. Tramite l'applicazione di criteri statistici e antropometrici, Bertillon elaborò un sistema di identificazione basato sulla comparazione delle caratteristiche somatiche, individuando una serie di misurazioni corporee ritenute sufficientemente distintive per identificare una persona con elevata probabilità.

¹⁴ Cfr. Facebook/Meta, *Managing your identity on Facebook with face recognition technology*, dicembre 2017: in questo comunicato viene ricordato che già nel 2010 era usata la tecnologia di riconoscimento facciale per suggerire l'identificazione di utenti nelle foto o nei video caricati.

¹⁵ Cfr. W. HU, T. TAN, L. WANG, S. MAYBANK, *A survey on visual surveillance of object motion and behaviors*, in IEEE transactions on systems, man, and cybernetics, vol. 34, n. 3, agosto 2004, pag. 335 ss.

¹⁶ Cfr. *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, in Human Rights Watch (www.hrw.org), 2019, pag. 12 s.

¹⁷ Cfr. *Francois Vidocq* in Encyclopaedia Britannica (www.britannica.com)

¹⁸ Cfr. *Bertillon Cards* in National library of medicine (www.nlm.gov) e *Alphonse Bertillon* in Encyclopaedia Britannica (www.britannica.com)

I sistemi contemporanei di riconoscimento facciale costituiscono l'esito più avanzato dell'evoluzione delle tecniche di identificazione personale, ma non coincidono con una mera intensificazione della videosorveglianza tradizionale. Il loro tratto qualificante risiede nella capacità di convertire il volto in informazione biometrica suscettibile di trattamento automatizzato, confronto e conservazione. È proprio questo passaggio dall'immagine al dato a determinare la specificità giuridica del fenomeno, poiché rende possibile un'identificazione potenzialmente seriale e diffusa, con rischi per i diritti fondamentali più penetranti di quelli riconducibili alla semplice osservazione visiva diretta dell'uomo¹⁹.

2. I sistemi di riconoscimento facciale e i dati biometrici: struttura e funzionamento

Per comprendere il funzionamento dei sistemi di riconoscimento facciale è necessario muovere dal ruolo dei dati biometrici, poiché tali tecnologie operano attraverso il trattamento automatizzato di informazioni relative alle caratteristiche fisiche o comportamentali degli individui.

La biometria viene generalmente definita come l'insieme delle tecniche che consentono il riconoscimento automatico delle persone sulla base delle loro caratteristiche biologiche o comportamentali²⁰. In questa prospettiva, i dati biometrici possono essere descritti come dati personali ottenuti mediante uno specifico trattamento tecnico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, come nel caso dell'immagine facciale, delle impronte digitali o della scansione dell'iride²¹.

I sistemi di riconoscimento facciale rappresentano una particolare applicazione delle tecnologie biometriche. I sistemi biometrici rappresentano la categoria più ampia delle tecniche di identificazione basate su caratteristiche fisiche o comportamentali

¹⁹ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 11 s.; cfr. W. HARTZOG, E. SELINGER, J.H. RHEE, *Normalizing facial recognition technology and the end of obscurity*, in *European Review of Digital Administration & Law – Erdal*, pag. 165 ss.; cfr. *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, in *FRA Focus* (www.fra.europa.eu), pag. 2

²⁰ Cfr. A.K. JAIN, A. ROSS, S. PRABHAKAR, *An Introduction to Biometric Recognition*, in *IEEE transaction on circuits and system for video technology*, vol. 14, n. 1, gennaio 2004 pag. 4

²¹ Nozione adottata dall'articolo 4, numero 14 del Regolamento (UE) 2016/679 e ripresa dall'articolo 3 del Regolamento (UE) 2024/1689; Cfr. C.D. FEDERICO e A.R. POPOLI, *Le definizioni*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli, 2019, pag. 66 s.

dell'individuo; il riconoscimento facciale, invece, utilizza l'analisi automatizzata delle caratteristiche del volto umano²². I sistemi biometrici possono fondarsi su diverse tipologie di dati, tra cui le impronte digitali, la scansione dell'iride o della retina, la voce o la geometria della mano. Il riconoscimento facciale, invece, utilizza tecniche di visione artificiale e algoritmi di apprendimento automatico per analizzare la struttura del volto umano, misurando le distanze e le proporzioni tra diversi punti caratteristici del viso al fine di generare una rappresentazione matematica del volto stesso²³.

La letteratura scientifica descrive tale rappresentazione come una sorta di “impronta facciale” che si ottiene tramite l'elaborazione di specifici punti di riferimento del volto – cd facial landmarks – e successivamente la sua conversione in un modello numerico che può essere confrontato con altri modelli presenti nei database biometrici²⁴. Il funzionamento di questi sistemi si articola in più fasi. In primo luogo, viene acquisita l'immagine di un volto tramite una fotografia o ripresa video. L'immagine così ottenuta costituisce il c.d. campione biometrico, a partire dal quale il sistema estrae specifiche caratteristiche facciali e le trasforma in una rappresentazione numerica, comunemente definita modello biometrico²⁵.

Il modello biometrico, quindi, consiste in una rappresentazione digitale delle caratteristiche facciali rilevate e viene usato per effettuare il confronto con altri modelli presenti all'interno di una banca dati. Le caratteristiche selezionate dagli algoritmi biometrici sono generalmente quelle ritenute relativamente stabili nel tempo, così da consentire il riconoscimento dell'individuo anche a distanza di anni e anche in presenza di variazioni dell'aspetto fisico²⁶.

²² Cfr. A. K. JAIN, A. ROSS, S. PRABHAKAR, *An Introduction to Biometric Recognition*, in IEEE transactions on circuits and systems for video technology, vol. 14, n. 1, gennaio 2004, pag. 6; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 32 s.

²³ Cfr. M. SAVVIDES, J. HEO, S.W. PARK, *Face Recognition*, in A.K. Jain, P. Flynn, A. Ross (a cura di), *Handbook of Biometrics*, Springer, 2008, pag. 44; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 32 s.

²⁴ Cfr. W.W. BLEDSOE, *Facial Recognition Project Report*, in Panoramic Research Inc., Marzo 1964, pag. 9 s.; cfr. M. SAVVIDES, J. HEO, S. W. PARK, *Face Recognition*, in A. K. Jain, P. Flynn, A. Ross (a cura di), *Handbook of Biometrics*, Springer, 2008, pag. 47

²⁵ Cfr. M. SAVVIDES, J. HEO, S.W. PARK, *Face Recognition*, in A. K. Jain, P. Flynn, A. Ross (a cura di), *Handbook of Biometrics*, Springer, 2008, pag. 45

²⁶ Cfr. M. SAVVIDES, J. HEO, S.W. PARK, *Face Recognition*, in A. K. Jain, P. Flynn, A. Ross (a cura di), *Handbook of Biometrics*, Springer, 2008, pag. 43

Una volta generato il modello biometrico, il sistema procede alla fase di confronto. In tale contesto è possibile distinguere due principali modalità operative:

- Se il sistema deve verificare l'identità di un individuo, come per consentire l'accesso a un dispositivo elettronico, viene effettuato un confronto detto "uno a uno" in cui il volto viene confrontato con un unico modello biometrico precedentemente registrato.
- Se il sistema deve identificare un individuo tra una pluralità di soggetti, come nell'ambito delle indagini di polizia, viene effettuato un confronto detto "uno a molti". In questo caso il modello biometrico ricavato dall'immagine viene confrontato con tutti i modelli presenti all'interno di una banca dati al fine di individuare eventuali corrispondenze²⁷.

In letteratura tale distinzione è generalmente descritta nei termini di autenticazione biometrica e identificazione biometrica. Nel primo caso il sistema si limita a verificare l'identità dichiarata da un individuo mediante il confronto con un unico modello biometrico precedentemente registrato. Nel secondo caso, invece, il sistema procede all'identificazione di un soggetto confrontando il campione biometrico con una pluralità di modelli presenti in una banca dati. Proprio quest'ultima modalità operativa è quella che solleva le maggiori criticità sotto il profilo della tutela dei diritti fondamentali, poiché consente potenzialmente l'identificazione automatica di individui all'interno di ampie popolazioni²⁸.

Il risultato del confronto viene espresso tramite un punteggio di similarità che rappresenta il grado di somiglianza tra due modelli biometrici. Il sistema, infatti, non fornisce quindi un'identificazione assoluta, ma indica una probabilità di corrispondenza tra i volti confrontati. La decisione sull'attendibilità del risultato

²⁷ Cfr. A.K. JAIN, A. ROSS, S. PRABHAKAR, *An Introduction to Biometric Recognition*, in IEEE transactions on circuits and systems for video technology, vol. 14, n. 1, gennaio 2004, pag. 5; cfr. J. L. WAYMAN, *Biometric Verification/Identification/Authentication/Recognition: The Terminology*, in S.Z. Li, A. Jain (a cura di), *Encyclopedia of Biometrics*, Springer, 2009, pag. 153 s.

²⁸ Cfr. J.L. WAYMAN, *Biometric Verification/Identification/Authentication/Recognition: The Terminology*, in S.Z. Li, A. Jain (a cura di), *Encyclopedia of Biometrics*, Springer, 2009, pag. 153; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 33 ss.

dipende anche dalla soglia di accettazione impostata, al di sopra della quale, la corrispondenza è considerata rilevante²⁹.

Proprio questo elemento costituisce uno dei principali fattori di criticità della tecnologia: le caratteristiche del volto umano, infatti, possono variare nel tempo in conseguenza di vari fattori come l'invecchiamento, variazioni dell'illuminazione o modifiche fisiche. Pertanto, volti appartenenti alla stessa persona possono risultare meno simili di quanto atteso, mentre volti di persone diverse possono presentare, a volte, livelli di somiglianza significativi³⁰.

Le applicazioni di queste tecnologie sono molto diffuse e disparate. I sistemi di riconoscimento facciale, ad esempio, vengono usati nei servizi bancari e finanziari per la verifica dell'identità degli utenti, nei dispositivi elettronici per l'accesso ai sistemi informatici, nei sistemi di pagamento digitali o nei sistemi di sicurezza domestica. Ulteriore ambito di impiego riguarda le attività di pubblica sicurezza, nel quale queste tecnologie possono essere usate come strumenti di supporto alle investigazioni e alle attività di law enforcement³¹.

Dal punto di vista operativo, inoltre, è possibile distinguere tra sistemi di riconoscimento facciale che operano in modalità differita, da quelli che operano in tempo reale: nel primo caso l'analisi delle immagini avviene successivamente alla loro acquisizione come nel caso dell'analisi di filmati di videosorveglianza, mentre nel secondo caso il sistema analizza i flussi video mentre vengono registrati e consente l'identificazione immediata di individui presenti nello spazio monitorato³².

La ricostruzione del funzionamento tecnico dei sistemi di riconoscimento facciale mostra che la rilevanza giuridica di tali strumenti non dipenda soltanto dalla raccolta

²⁹ Cfr. A.K. JAIN, A. ROSS, *Introduction to Biometrics*, in Handbook of Biometrics, Springer, 2008, pag. 5, 8; cfr. M. SAVVIDES, J. HEO, S. W. PARK, *Face Recognition*, in A.K. Jain, P. Flynn, A. Ross (a cura di), Handbook of Biometrics, Springer, 2008, pag. 43

³⁰ Cfr. A.K. JAIN, A. ROSS, *Introduction to Biometrics*, in A.K. Jain, P. Flynn, A. Ross (a cura di), Handbook of Biometrics, Springer, 2008, pag. 6 s. e 15 s.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 32

³¹ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 11 s. e 22 s.; cfr. A.K. JAIN, A. ROSS, S. PRABHAKAR, *An Introduction to Biometric Recognition*, in IEEE transactions on circuits and systems for video technology, vol. 14, n. 1, gennaio 2004, pag. 4 e 12

³² Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 25, 140

dell'immagine, ma soprattutto dalla trasformazione del volto in un modello biometrico suscettibile di confronto automatizzato. È questo passaggio a spiegare perché il riconoscimento facciale non possa essere considerato una tecnologia neutra: le sue modalità operative incidono direttamente sull'intensità del rischio giuridico e rendono necessario interrogarsi sui diritti fondamentali coinvolti³³.

3. La ridefinizione dei diritti fondamentali nell'era della sorveglianza biometrica

3.1 *L'incidenza del riconoscimento facciale sui diritti individuali*

L'impiego dei sistemi di riconoscimento facciale impone di verificare come le categorie tradizionali dei diritti fondamentali possano applicarsi a tecnologie che non erano prevedibili al momento della stesura della Carta costituzionale repubblicana. La Costituzione del 1948, infatti, non contiene espressi riferimenti alla protezione dei dati personali, ai dati biometrici o all'identificazione automatizzata degli individui, ma costruisce un sistema di tutele basato sulla centralità della persona, sulla garanzia dei suoi diritti inviolabili e sul limite che questi pongono all'esercizio dei poteri pubblici e privati.

In tale prospettiva, l'articolo 2 della Costituzione assume un ruolo centrale in quanto riconosce e garantisce i diritti inviolabili dell'uomo sia come singolo, sia nelle formazioni sociali in cui si svolge la sua personalità. Ad esso si ricollega l'articolo 3 della Costituzione che non si limita a sancire l'eguaglianza formale dinanzi alla legge, ma affida alla Repubblica il compito di rimuovere gli ostacoli che impediscono il pieno sviluppo della persona umana. Altre garanzie specifiche sono poi previste dagli articoli 13, 14 e 15 della Costituzione relativi alla libertà personale, all'inviolabilità del domicilio e alla libertà e segretezza delle comunicazioni, che esprimono l'esigenza di proteggere la persona da interferenze arbitrarie nella propria sfera fisica, privata e relazionale³⁴.

³³ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 25; cfr. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, adottato il 26 aprile 2023, pag. 5 s.; cfr. FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, pag. 3, 24

³⁴ V. Costituzione italiana, artt. 2, 3, 13, 14, 15; cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 46 ss.; cfr. S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Jovene editore, 2018, pag. 52 ss.; cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati*

La struttura aperta e personalista della Carta ha consentito a dottrina e giurisprudenza di ricondurre nuove esigenze di tutela della persona entro il sistema costituzionale, anche in assenza di una previsione testuale espressa. In tal senso, l'evoluzione tecnologica non ha imposto la creazione di diritti estranei al sistema costituzionale, ma ha richiesto una rilettura delle garanzie esistenti alla luce di nuovi strumenti di conoscenza e controllo. Il riconoscimento facciale si colloca proprio in questa traiettoria: non introduce solo una modalità più efficiente di identificazione, ma rende possibile la conversione del volto in un dato biometrico suscettibile di essere conservato, confrontato e collegato ad altre informazioni. Ne deriva che i diritti coinvolti devono essere letti come un sistema unitario di garanzie poste a protezione della persona contro forme di osservazione e identificazione sempre più pervasive³⁵.

Da ciò, discende la necessità di muovere dal diritto alla riservatezza e dalla sua progressiva evoluzione verso il diritto alla protezione dei dati personali: il riconoscimento facciale non incide solo sulla possibilità di mantenere segreti determinati aspetti della vita privata, ma sulla facoltà della persona di conservare un controllo effettivo sulle informazioni che la riguardano, comprese quelle ricavate dal corpo e idonee a renderla univocamente identificabile³⁶.

Nel nostro ordinamento, il diritto alla riservatezza si è affermato progressivamente come proiezione della tutela della persona, pur in assenza di una disposizione espressamente dedicata alla privacy. In una prima fase, esso è stato ricostruito soprattutto come pretesa dell'individuo a mantenere riservati aspetti della propria vita privata, sottraendoli a forme di conoscenza, divulgazione o esposizione non giustificate. Questa impostazione richiamava la tradizionale concezione di privacy come diritto a essere lasciati soli di matrice Ottocentesca: in questa accezione, la

personali, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 12 s.

³⁵ Cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 46 ss.; cfr. S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Jovene editore, 2018, pag. 52 ss.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 11 ss., 119 ss.

³⁶ Cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 12 s.; cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 46 ss.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 119 ss.

riservatezza, esprime l'esigenza di delimitare uno spazio personale sottraendolo allo sguardo altrui e alle intrusioni non autorizzate nella vita privata³⁷.

Il diritto alla riservatezza ha trovato un primo riconoscimento significativo nella giurisprudenza della Corte di cassazione che, con la sentenza n. 2129 del 1975, ha riconosciuto la riservatezza come diritto della personalità, collegandola al sistema costituzionale di tutela della persona e alla necessità di proteggere la sfera privata da indebite ingerenze. Successivamente, la stessa Corte con la sentenza n. 5658 del 1998 ha consolidato questa impostazione valorizzando la riservatezza come interesse giuridicamente tutelato nei confronti di intrusioni nella vita privata e familiare, anche tramite il ricorso alla clausola generale di cui all'articolo 2043 del Codice civile relativa al danno ingiusto. In questo modo, la riservatezza è stata progressivamente ricondotta non solo a un'esigenza morale o sociale, ma a una posizione giuridica soggettiva pienamente tutelabile³⁸.

Trattandosi, tuttavia, di una concezione in negativo di privacy, con l'evoluzione tecnologica ne sono emersi i rispettivi limiti: con lo sviluppo delle banche dati e delle tecnologie di raccolta automatizzata delle informazioni, il problema non è più rappresentato solo dalla divulgazione di fatti intimi o segreti, ma dalla possibilità di raccogliere, conservare, incrociare e utilizzare una pluralità di dati riferibili a una persona. Di conseguenza, la tutela della riservatezza si è trasformata in un'esigenza di controllo sulle informazioni personali, quindi non si tratta più solo di impedire ingerenze esterne nella sfera privata, ma di garantire alla persona la possibilità di conoscere e governare la circolazione dei dati che la riguardano³⁹.

³⁷ Cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 46 ss. L'espressione diritto alla privacy nasce diritto a essere lasciati soli – the right to be let alone. Tale formula fu elaborata nel 1890 dagli avvocati statunitensi S. Warren e L. Brandeis nel saggio “the right to privacy” pubblicato sulla Harvard Law Review come critica all'invasione della stampa scandalistica dell'epoca. In origine, quindi la privacy era intesa soprattutto come diritto di escludere la propria vita privata dall'attenzione altrui e dall'ingerenza della stampa.

³⁸ Cfr. Corte cass., sez. I, 27 maggio 1975, n. 2129, in *Il Foro italiano*, 1976, I, c. 2896 ss.; cfr. Corte cass., sez. III, 9 giugno 1998, n. 5658, in *Il Foro italiano*, 1998, I, c. 2387 ss.; cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 46 ss.

³⁹ Cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 46 ss.; cfr. S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Jovene editore, 2018, pag. 52 ss.; cfr. L.A. BYGRAVE, *EU data protection law*, Wolters Kluwer, 2002, pag. 167 s.

Questa evoluzione ha trovato un primo riscontro nella legge n. 675/1996 con cui l'ordinamento italiano, in attuazione della Direttiva 95/46/CE, ha introdotto una prima disciplina organica in materia di trattamento dei dati personali successivamente confluita nel c.d. Codice privacy del 2003. Si è così passati da una concezione di riservatezza come tutela statica della sfera privata, alla protezione dei dati personali come garanzia dinamica dell'identità e dell'autodeterminazione individuale. La protezione dei dati personali, infatti, riguarda ogni informazione riferibile a una persona identificata o identificabile nella misura in cui il suo trattamento possa incidere sulla libertà, sull'identità e sulle possibilità di autodeterminazione dell'interessato⁴⁰. Questo passaggio trova ulteriore conferma nell'ordinamento europeo che ha riconosciuto la protezione dei dati personali come diritto fondamentale autonomo. L'articolo 7 della Carta dei diritti fondamentali dell'Unione europea tutela espressamente il rispetto della vita privata e familiare, mentre l'articolo 8 riconosce il diritto alla protezione dei dati personali; in tale quadro si aggiunge l'articolo 16 del TFUE che attribuisce a tale diritto un fondamento specifico nel diritto primario europeo. La Corte di giustizia, inoltre, nella sentenza *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen* ha chiarito il rapporto tra tali garanzie affermando che il diritto al rispetto della vita privata nella sua dimensione di protezione dei dati personali, riguarda ogni informazione relativa a una persona fisica identificata o identificabile. Quindi, la protezione dei dati personali si configura come diritto autonomo, sebbene strettamente collegato alla vita privata, e ogni eventuale limitazione deve rispettare i requisiti dell'articolo 52, paragrafo 1 della stessa Carta, e pertanto deve essere prevista dalla legge, rispettare il contenuto essenziale dei diritti coinvolti e risultare proporzionata rispetto a finalità di interesse generale⁴¹.

⁴⁰ V. l. 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali); v. d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali); cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 12 s.; cfr. L.A. BYGRAVE, *EU data protection law*, Wolters Kluwer, 2002, pag. 167 s.

⁴¹ V. Carta dei diritti fondamentali dell'Unione europea, artt. 7, 8; v. Trattato sul funzionamento dell'Unione europea, art. 16; cfr. Corte di Giustizia, Grande Sezione, sent. 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, in Eur-Lex (www.eur-lex.europa.eu), punti 52 ss., 65 ss., 77 ss.; cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 12 s.

Nell'ambito dei sistemi di riconoscimento facciale, tale evoluzione assume un rilievo peculiare in quanto l'interferenza con il diritto in esame risiede nella trasformazione del volto in una chiave tecnica di identificazione, confronto e tracciamento. Il passaggio da mera visibilità di un volto, a una sua elaborazione biometrica mostra come la protezione dei dati personali sia oggi chiamata a operare quale garanzia dinamica della persona in quanto non tutela solo ciò che deve rimanere nascosto, ma anche il potere della persona di non essere resa stabilmente identificabile, classificabile e collegabile ad altri dati in assenza di una base giuridica adeguata e di garanzie proporzionate⁴².

Nel riconoscimento facciale, il passaggio da protezione dei dati personali a disciplina dei dati biometrici è decisivo, infatti, la tecnologia non si limita a usare una foto come semplice immagine, ma sottopone il volto a uno specifico trattamento tecnico volto a estrarne caratteristiche misurabili e a convertirle in una rappresentazione numerica: il volto viene trasformato in un modello biometrico ovvero in un'informazione idonea a essere conservata, confrontata con altri modelli e, potenzialmente, usata per diversi scopi⁴³.

Tale passaggio assume rilievo non solo sul piano della protezione dei dati personali, ma anche sul piano più ampio della tutela della persona. Il volto, infatti, non è un elemento neutro: è parte del corpo, ma è anche uno dei principali strumenti con cui l'individuo si presenta agli altri, viene riconosciuto e costruisce la propria identità nella dimensione sociale. La sua conversione in dato biometrico determina una trasformazione qualitativa perché ciò che normalmente appartiene alla relazione interpersonale viene reso disponibile a operazioni automatizzate di misurazione, confronto e classificazione⁴⁴. In tale prospettiva, viene in rilievo anche il principio di

⁴² Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 119 ss.; cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 46 ss.; cfr. FRA Focus, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 2

⁴³ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 32 s., 119 ss.; cfr. A.K. JAIN, A. ROSS, S. PRABHAKAR, *An introduction to biometric recognition*, in IEEE transaction on circuits and system for video technology (www.ieee-cas.org), vol. 14, n.1, gennaio 2004, pag. 4 ss.

⁴⁴ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 140 ss.; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 179 s.

dignità umana: nel nostro ordinamento emerge dagli articoli 2 e 3 della Costituzione che impongono di considerare la persona non come mero oggetto di trattamento tecnico o amministrativo, ma come soggetto titolare di una sfera di identità, libertà e autodeterminazione che deve restare protetta anche dinanzi alle nuove forme di identificazione automatizzata⁴⁵.

Il rischio posto dal riconoscimento facciale, quindi, non consiste solo nella raccolta di un dato personale, ma nella possibilità che un tratto identitario venga stabilmente trasformato in strumento di riconoscibilità tecnica. Ciò non significa che ogni impiego di tali tecnologie determini in automatico una violazione della dignità umana, ma impone di valutare con rigore le condizioni in cui il volto viene acquisito, elaborato e usato. La dignità, in questo senso, opera come criterio di limite in quanto impedisce di considerare il corpo come semplice supporto dell'identificazione e richiede che l'uso della tecnologia non riduca la persona a un insieme di caratteristiche misurabili e classificabili⁴⁶.

L'impiego di tali tecnologie in ambito investigativo pone, infine, un ulteriore problema connesso alla presunzione di innocenza e alle garanzie procedurali della persona sottoposta a controllo. L'articolo 27, comma 2, della Costituzione stabilisce che l'imputato non sia considerato colpevole sino alla condanna definitiva; sul piano sovranazionale, il medesimo principio trova riconoscimento nell'articolo 6, paragrafo 2, della CEDU e nell'articolo 48 della Carta dei diritti fondamentali dell'Unione europea. Pur riferendosi propriamente alla posizione dell'imputato nel processo penale, tale principio esprime più ampiamente l'esigenza che l'intervento dell'autorità pubblica non si fondi su presunzioni automatiche o meccanismi di sospetto non adeguatamente verificati⁴⁷. Nel contesto del riconoscimento facciale, il problema

⁴⁵ V. Costituzione italiana, artt. 2, 3; v. art. 1 CDFUE; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 140 ss.; cfr. S. Rodotà, *Il diritto di avere diritti*, editori Laterza, 2012, pag. 158 ss.

⁴⁶ Cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 180 ss.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 140 ss.

⁴⁷ V. Costituzione italiana, art. 27, co. 2; v. Convenzione europea dei diritti dell'uomo, art. 6 par. 2; v. Carta dei diritti fondamentali dell'Unione europea, art. 48; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 154 ss.

nasce dal fatto che l'output del sistema non equivale a una certezza identificativa, ma consiste in una corrispondenza probabilistica o in una lista di possibili candidati. Il risultato algoritmico dovrebbe quindi essere inteso come mero elemento di orientamento investigativo che necessita di riscontri e verifiche umane, ma se viene recepito in modo acritico dall'autorità procedente, il rischio è che una probabilità tecnica venga trasformata in sospetto giuridicamente rilevante, con conseguenze concrete sulla persona⁴⁸. Questo rischio appare particolarmente delicato in quanto l'apparenza di oggettività della tecnologia può indurre a sovrastimare l'affidabilità dell'esito prodotto dal sistema. L'identificazione biometrica, proprio perché fondata su calcoli automatizzati e su una rappresentazione numerica del volto, può essere percepita come più neutra o certa rispetto ad altre forme di accertamento. Il risultato fornito dal sistema dipende da una serie di elementi e il controllo umano non può dunque limitarsi a una ratifica formale dell'output algoritmico, ma deve consistere in una valutazione critica e documentabile⁴⁹. In tale prospettiva, le garanzie procedurali assumono un ruolo centrale: l'uso del riconoscimento facciale dovrebbe essere accompagnato da regole chiare sulla tracciabilità degli accessi, sulla conservazione dei risultati, sulla formazione degli operatori, sulla verifica delle corrispondenze e sulla possibilità di contestare l'esito del trattamento. La persona erroneamente identificata, infatti, non dovrebbe trovarsi nella posizione di dover dimostrare che la tecnologia si è sbagliata, al contrario deve essere la pubblica autorità a fondare ogni ulteriore attività investigativa o restrittiva su elementi autonomi, verificabili e proporzionati⁵⁰. Questa esigenza trova conferma anche nel più recente quadro europeo sull'intelligenza artificiale che insiste sulla necessità di una sorveglianza umana effettiva nei sistemi ad

⁴⁸ Cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 197 ss.; cfr. J.D. TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in G.D. Paolo, L. Pressacco (a cura di), *Intelligenza artificiale e processo penale*, 2022, pag. 39 s.

⁴⁹ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 154 ss., 219 ss.; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 196 s.; cfr. FRA Focus, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 27 s.

⁵⁰ Cfr. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, aprile 2023, pag. 14 ss.; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 196 ss.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 154 ss.

alto rischio ed esclude, in merito all'identificazione biometrica, che decisioni produttive di effetti giuridici negativi possano essere assunte unicamente sulla base dell'output del sistema. Il nodo centrale, quindi, non è negare l'impiego del riconoscimento facciale nelle indagini, ma impedire che operi come una scorciatoia probatoria o come meccanismo automatico di costruzione del sospetto⁵¹.

Ne deriva che la presunzione di innocenza e le garanzie procedurali impongono di mantenere una netta distinzione tra identificazione algoritmica e accertamento giuridico in concreto. Il riconoscimento facciale, al più, orienta l'attività investigativa ma non dovrebbe sostituire la valutazione dell'autorità o fondare da solo misure negative nei confronti della persona: solo in presenza di controlli umani effettivi, riscontri indipendenti e criteri di utilizzo trasparenti è possibile evitare che l'automazione dell'identificazione trasformi un dato probabilistico in una presunzione di responsabilità⁵².

3.2 L'incidenza del riconoscimento facciale sui diritti partecipativi e sulla dimensione democratica

Una tecnologia capace di rendere il volto stabilmente identificabile non incide solo sulla dimensione informativa della persona, ma può riflettersi anche sul modo in cui si muove, espone e partecipa allo spazio pubblico. Da ciò discende la necessità di considerare, accanto alla riservatezza, alla protezione dei dati personali e alla dignità umana, anche la libertà di circolazione, di riunione, di associazione e di manifestazione del pensiero⁵³.

L'impiego dei sistemi di riconoscimento facciale può incidere sull'esercizio concreto delle libertà costituzionali che presuppongono la libera presenza della persona nello

⁵¹ V. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*, art. 14, 26 par. 10; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 196 s.

⁵² Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 154 ss.; cfr. J.D. TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in G.D. Paolo, L. Pressacco (a cura di), *Intelligenza artificiale e processo penale*, 2022, pag. 39 s.; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 197 ss.

⁵³ Cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 181 s.; cfr. FRA Focus, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 24

spazio pubblico. Vengono in rilievo, nello specifico, la libertà di circolazione, di riunione, di associazione e di manifestazione del pensiero tutelate dagli articoli 16, 17, 18 e 21 della Costituzione. Tali libertà non proteggono solo singole facoltà individuali, ma garantiscono la possibilità della persona di muoversi, incontrarsi, associarsi, partecipare alla vita collettiva ed esprimere la propria posizione nello spazio democratico⁵⁴.

Tali tecnologie possono incidere su tali libertà tramite una forma indiretta di condizionamento, infatti, la possibilità di essere identificati automaticamente mentre ci si trova in un determinato luogo, si partecipa a una manifestazione, si accede a un edificio pubblico o si incontra una persona, può indurre le persone a modificare i propri comportamenti, evitando condotte perfettamente lecite ma percepite come sensibili. Il problema, dunque, non riguarda solo l'eventuale abuso dello strumento, ma anche l'effetto che la mera possibilità di identificazione biometrica può produrre sulla spontaneità dell'agire individuale⁵⁵. In questa prospettiva si colloca il fenomeno del chilling effect, ovvero l'effetto di autocensura che la sorveglianza può determinare sull'esercizio delle libertà fondamentali. La persona, pur formalmente libera di circolare, riunirsi, associarsi o manifestare il proprio pensiero, può essere scoraggiata dall'esercizio di tali diritti se percepisce lo spazio pubblico come un luogo in cui ogni movimento può essere registrato, identificato e poi ricondotto alla propria identità. La libertà non viene compressa solo quando è vietata, ma anche quando il contesto tecnologico in cui si vive diviene tale da produrre pressione, controllo o conformazione dei comportamenti⁵⁶.

⁵⁴ V. Costituzione italiana, artt. 16, 17, 18, 21; v. Convenzione europea dei diritti dell'uomo, artt. 10, 11; v. Carta dei diritti fondamentali dell'Unione europea, artt. 11, 12; cfr. FRA Focus, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 24

⁵⁵ Cfr. N. RICHARDS, *The dangers of surveillance*, in Harvard Law Review, vol. 126, n. 7, Maggio 2013, pag. 1935 s.; cfr. EDPB-EDPS, *Joint opinion 5/2021 for a regulation of the European Parliament and the Council laying down harmonized rules on artificial intelligence*, pag. 2 s.; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 181 s.

⁵⁶ Cfr. N. RICHARDS, *The dangers of surveillance*, in Harvard Law Review, vol. 126, n. 7, maggio 2013, pag. 1946 ss.; cfr. EDPB-EDPS, *Joint opinion 5/2021 for a regulation of the European Parliament and the Council laying down harmonized rules on artificial intelligence*, pag. 2 s.; cfr. J.D. TORRE, *Quale spazio per i tools di riconoscimento facciale nella giustizia penale?*, in G.D. Paolo, L. Pressacco (a cura di), *Intelligenza artificiale e processo penale*, 2022, pag. 39 s.; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 181 s.

Sotto questo profilo, il riconoscimento facciale determina un salto di qualità rispetto alla videosorveglianza classica: le telecamere permettono di osservare e/o registrare immagini, ma i sistemi biometrici consentono di associare quelle immagini a delle identità determinate. Il problema, dunque, non è solo quello di essere visti, ma quello di essere riconoscibili e collegabili ad altre informazioni: tale passaggio rende i sistemi di riconoscimento facciale problematici per l'esercizio delle libertà democratiche⁵⁷. Il profilo assume rilievo anche alla luce della giurisprudenza europea. La Corte europea dei diritti dell'uomo ha più volte evidenziato come le forme di sorveglianza e di raccolta sistematica di dati personali da parte delle autorità pubbliche possano incidere sul rapporto tra individuo e potere. In questa linea si colloca anche il caso *Glukhin c. Russia* che mostra come l'identificazione biometrica nello spazio pubblico possa incidere sulla partecipazione democratica, soprattutto se utilizzata per ricondurre a identità determinate comportamenti espressivi o politicamente sensibili⁵⁸.

Ne deriva che tali sistemi non producono solo un rischio puntuale di violazione della privacy o della protezione dei dati personali, ma possono modificare la qualità dello spazio pubblico. Se una persona sa di poter essere costantemente identificato cambia il rapporto che ha sia con lo spazio urbano, sia con le autorità: la sorveglianza biometrica diffusa può incidere sulle condizioni complessive di esercizio delle libertà fondamentali⁵⁹.

Le ricadute delle tecnologie in esame sulle libertà fondamentali si collegano anche al principio di eguaglianza e al divieto di discriminazione. L'articolo 3 della Costituzione, oltre a imporre di evitare trattamenti differenziati esplicitamente discriminatori, richiede anche di considerare gli effetti concreti che determinate scelte normative,

⁵⁷ Cfr. W. HARTZOG, E. SELINGER, J.H. RHEE, *Normalizing facial recognition technology and the end of obscurity*, in *European review of digital administration & law*, 2025, pag. 166 s.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 119 ss.; cfr. FRA Focus, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 3, 24

⁵⁸ Cfr. Corte EDU, *Grande Camera*, sent. 25 maggio 2021, *Big Brother Watch and Others c. Regno Unito*, ric. nn. 58170/13, 62322/14, 24960/15, in Hudoc (www.hudoc.echr.coe.int); cfr. Corte EDU, sez. III, sent. 4 luglio 2023, *Glukhin c. Russia*, in Hudoc (www.hudoc.echr.coe.int) ric. n. 11519/20, parr. 82, 83, 88, 89; cfr. M. ZALNIERIUTE, *Glukhin c. Russia. App. n. 11519/20. Judgment*, in *American Journal of international law*, 2023, pag. 695 ss.

⁵⁹ Cfr. N. RICHARDS, *The dangers of surveillance*, in *Harvard Law Review*, vol. 126, n. 7, Maggio 2013, pag. 1935 s.; cfr. EDPB-EDPS, *Joint opinion 5/2021 for a regulation of the European Parliament and the Council laying down harmonized rules on artificial intelligence*, pag. 11

amministrative o tecnologiche possono produrre su gruppi diversi di persone⁶⁰. Questo profilo assume particolare rilievo perché spesso la tecnologia viene presentata come neutrale in quanto fondata su procedure automatizzate di misurazione, comparazione e calcolo probabilistico, tuttavia, la neutralità tecnica non coincide necessariamente con la neutralità giuridica o sociale del risultato. Il funzionamento di tali sistemi, infatti, dipende dalla qualità dei dati utilizzabili, dalla rappresentatività dei dataset di addestramento, dalle condizioni concrete di acquisizione dell'immagine e dalla composizione delle banche dati impiegate per il confronto biometrico. Ne deriva che uno strumento apparentemente uniforme può produrre effetti differenziati esponendo alcune categorie di persone a un rischio maggiore di errore, identificazione o controllo⁶¹.

Molti studi hanno evidenziato come i sistemi di riconoscimento facciale possano presentare livelli di accuratezza diversi a seconda delle caratteristiche demografiche degli individui analizzati. Nello specifico, alcune ricerche hanno mostrato tassi di errore più elevati nei confronti di persone appartenenti a minoranze etniche e di sesso femminile. Le cause di queste distorsioni risiedono spesso nella composizione dei dataset usati per l'addestramento degli algoritmi che possono riflettere squilibri già presenti nella società e riprodurli nei risultati prodotti dai sistemi automatizzati⁶².

Il problema diviene particolarmente rilevante quando tali tecnologie vengono impiegate dalle autorità pubbliche, specie nell'ambito della sicurezza pubblica. In questi contesti, il falso positivo non rappresenta un semplice errore tecnico, ma può produrre conseguenze concrete sulla persona erroneamente identificata: controlli più intensi, verifiche di polizia, perquisizioni, interrogatori o arresti ingiustificati. Il rischio

⁶⁰ V. Costituzione italiana, art. 3; v. Convenzione europea dei diritti dell'uomo, art. 14; v. Carta dei diritti fondamentali dell'Unione europea, art. 21; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 219 ss.

⁶¹ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 219 ss.; cfr. FRA Focus, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 27 s.; cfr. Council of Europe, *Guidelines on facial recognition*, giugno 2021, pag. 8, 15

⁶² Cfr. J. BUOLAMWINI, T. GEBRU, *Gender shades: intersectional accuracy disparities in commercial gender classification*, in *Proceedings of machine learning research*, vol. 81, 2018, pag. 3, 8; cfr. P. GROTH, M. NGAN, K. HANAOKA, *Face recognition vendor test (FRVT), part 3: demographic effects*, NIST Interagency Report 8289, 2019, pag. 2, 7 s.; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 183

discriminatorio, quindi, non deriva solo dalla diversa performance dell'algoritmo, ma anche dal modo in cui l'errore tecnico viene recepito dall'apparato pubblico e trasformato in sospetto investigativo⁶³.

Il profilo discriminatorio può, inoltre, derivare dal funzionamento interno dell'algoritmo e dalla composizione della banca dati rispetto alla quale il confronto viene effettuato. Una banca dati non rappresentativa della popolazione generale, o alimentata prevalentemente da precedenti attività di polizia o di identificazione amministrativa, può determinare un'esposizione diseguale al controllo biometrico. In queste ipotesi anche un sistema formalmente neutro può produrre effetti indirettamente discriminatori, poiché i gruppi maggiormente presenti nell'archivio risultano più esposti alla possibilità di comparire tra i candidati restituiti dal sistema, di essere sottoposti a ulteriori verifiche o di subire le conseguenze di un falso positivo⁶⁴.

Alla luce di questi elementi, il principio di eguaglianza impone di valutare il riconoscimento facciale non solo in termini di prestazione tecnica complessiva, ma anche in relazione agli effetti differenziati che può produrre sui vari gruppi sociali. Una tecnologia, infatti, può essere formalmente uniforme nel funzionamento, e al contempo diseguale nei suoi effetti se si innesta su dataset, archivi o prassi amministrative già caratterizzati da squilibri. Il divieto di discriminazione richiede, pertanto, che l'impiego dei sistemi biometrici sia accompagnato da controlli rigorosi sulla qualità dei dati, sulla rappresentatività dei dataset, sulla misurazione dei falsi positivi e sulla possibilità di verifica umana effettiva⁶⁵.

⁶³ Cfr. FRA Focus, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 27 s.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 219 ss.; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 183 ss.

⁶⁴ Cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 192 s.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 219 ss.

⁶⁵ V. Costituzione italiana, art. 3; v. Carta dei diritti fondamentali dell'Unione europea, art. 21; v. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*, artt. 14, 26 par. 10; cfr. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, Aprile 2023, pag. 14 ss.; A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 196 s.

Le considerazioni svolte mostrano come il riconoscimento facciale non incida solo su singole posizioni soggettive considerate isolatamente, ma possa modificare le condizioni complessive in cui la persona esercita i propri diritti: riservatezza, protezione dei dati personali, dignità, eguaglianza e le libertà costituzionali rilevano come parti di uno stesso problema, ovvero la progressiva trasformazione dello spazio fisico e digitale in un ambiente in cui l'identità personale può essere rilevata, verificata e collegata ad altri dati in modo automatizzato⁶⁶. In questa prospettiva può essere richiamata la categoria dell'ambiente digitale e dell'informazionale salubre. Il riferimento non va inteso come affermazione dell'esistenza di un autonomo diritto già consolidato, né come sovrapposizione meccanica tra ambiente naturale e spazio digitale, piuttosto può essere usato in senso analogico per evidenziare che la tutela della persona non dipende solo dal divieto di singole interferenze illegittime, ma anche dalla qualità complessiva degli ambienti digitali e materiali in cui la personalità si forma e manifesta⁶⁷. Il fondamento di tale analogia può essere rinvenuto, da un lato, nella tradizionale elaborazione del diritto all'ambiente salubre, quale proiezione del diritto alla salute e della tutela del contesto di vita della persona; dall'altro lato, nella dottrina del costituzionalismo digitale, che ha evidenziato come gli ambienti tecnologicamente mediati non siano spazi neutri, ma luoghi nei quali si esercitano diritti, si producono relazioni sociali e si manifestano nuovi poteri pubblici e privati. In questa direzione si colloca anche l'impostazione del Consiglio d'Europa, secondo cui i diritti umani e le libertà fondamentali devono trovare applicazione anche online, non venendo meno per il solo fatto che la persona agisca, comunichi o sia osservata in un ambiente dematerializzato⁶⁸.

⁶⁶ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale scientifica, 2021, pag. 119 ss., 140 ss., 154 ss., 219 ss.; cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 180 ss.

⁶⁷ Cfr. Corte cass., Sez. Un., 6 ottobre 1979, n. 5172, in *Il Foro italiano*, 1979, I, c. 2302 ss.; cfr. C.D. GIUSTINA, *Il diritto all'ambiente nella costituzione italiana*, in *Ambiente diritto* (www.ambientediritto.it), 2020, pag. 1 ss.; cfr. P. CARPINETO, *La tutela dell'ambiente nella costituzione italiana*, 2016, pag. 5 ss.

⁶⁸ Cfr. E. CELESTE, *Digital constitutionalism: a new systematic theorization*, in *International review of law, computers & technology*, 33(11), 2019, pag. 77 ss.; cfr. O. POLLICINO, *Tutela dei diritti fondamentali nell'era digitale e contesto valoriale: una indagine transatlantica*, in *MediaLaws* (www.medialaws.eu), 2018, pag. 39 ss.; cfr. Council of Europe, Committee of Ministers, *Recommendation CM/Rec(2014)6 to member States on a Guide to human rights for internet users*, aprile 2014; cfr. S. RODOTÀ, *Una costituzione per internet?*, in *Il Mulino - Rivisteweb*, n. 3/2010, pag. 337 ss.

Applicata al riconoscimento facciale, questa prospettiva permette di cogliere un profilo ulteriore rispetto alla sola liceità del singolo trattamento biometrico. La sorveglianza biometrica diffusa, infatti, può contribuire alla formazione di un ambiente in cui l'individuo è stabilmente osservabile, identificabile e potenzialmente tracciabile. Il rischio non è soltanto quello della violazione puntuale della privacy o della protezione dei dati personali, ma quello di un deterioramento della qualità democratica dello spazio a causa del fenomeno del chilling effect⁶⁹. Il richiamo all'ambiente digitale salubre, quindi, non sostituisce le categorie giuridiche tradizionali, ma le integra. Esso permette di leggere il riconoscimento facciale come tecnologia capace di incidere non soltanto sulla singola posizione individuale, bensì sulle condizioni complessive di esercizio della libertà personale, della partecipazione democratica e dell'autodeterminazione. Per tale ragione, una disciplina adeguata di tali sistemi dovrebbe tenere conto non solo della base giuridica del trattamento, dell'accuratezza dell'algoritmo e della verifica umana, ma anche dell'impatto sistemico che l'identificazione biometrica produce sull'ambiente in cui la persona sviluppa la propria identità⁷⁰.

⁶⁹ Cfr. N. RICHARDS, *The dangers of surveillance*, in Harvard law review, vol. 126, n. 7, Maggio 2013, pag. 1935 s., 1946 ss.; cfr. W. HARTZOG, E. SELINGER, J.H. RHEE, *Normalizing facial recognition technology and the end of obscurity*, in European review of digital administration & law, 2025, pag. 165 ss.; cfr. FRA Focus, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 24

⁷⁰ Cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 180 ss.; cfr. E. CELESTE, *Digital constitutionalism: a new systematic theorization*, in International review of law, computers & technology, 33(11), 2019, pag. 76 ss.; cfr. O. POLLICINO, *Tutela dei diritti fondamentali nell'era digitale e contesto valoriale: una indagine transatlantica*, in MediaLaws (www.medialaws.eu), 2018, pag. 39 ss.; cfr. EDPB-EDPS, *Joint opinion 05/2021 for a regulation of the European Parliament and the Council laying down harmonized rules on artificial intelligence*, pag. 11

Capitolo 2

Il quadro normativo europeo e italiano

SOMMARIO: 1. La disciplina europea del riconoscimento facciale tra protezione dei dati personali e regolazione dell'intelligenza artificiale. – 1.1. Tutela dei dati biometrici e principi del trattamento alla luce del GDPR. – 1.2. Requisiti e obblighi per i sistemi di intelligenza artificiale alla luce dell'AI Act. – 2. Le autorità di controllo nel sistema europeo di protezione dei dati. – 3. Italia: dal Codice privacy alla legge 132/2025. – 4. Il Garante per la protezione dei dati personali e i sistemi di riconoscimento facciale – un'analisi per casi. – 4.1. Il caso SARI – tra l'investigazione e l'identificazione biometrica in tempo reale. – 4.1.1. I più recenti sviluppi dell'attuazione nazionale dell'AI Act in materia di identificazione biometrica. – 4.2. Il caso Clearview AI. – 4.3. Le sperimentazioni del riconoscimento facciale negli aeroporti – faceboarding. – 4.4. Il riconoscimento facciale e i rapporti tra privati. – 4.5. Tra prudenza e principi, l'approccio del Garante privacy al riconoscimento facciale.

1. *La disciplina europea del riconoscimento facciale tra protezione dei dati personali e regolazione dell'intelligenza artificiale*

1.1 *Tutela dei dati biometrici e principi del trattamento alla luce del GDPR*

Il Regolamento (UE) 679/2016 – cd GDPR – si colloca nel solco dell'articolo 8 della CDFUE e dell'articolo 16 del TFUE che configurano la protezione dei dati personali come diritto fondamentale autonomo, sebbene connesso – come già visto – con il diritto al rispetto della vita privata⁷¹.

I Considerando introduttivi chiariscono, infatti, che il trattamento dei dati personali deve essere al servizio dell'uomo e che il relativo diritto alla protezione dei dati non è una prerogativa assoluta, dovendo essere bilanciato con gli altri diritti fondamentali⁷².

Alla base del Regolamento abbiamo un modello sostanzialistico che si esprime nella responsabilizzazione del titolare e nella necessità di soppesare obblighi e garanzie in funzione del rischio per i diritti e le libertà delle persone fisiche⁷³. In questa

⁷¹ V. Carta dei diritti fondamentali dell'Unione europea, art. 8; v. Trattato sul funzionamento dell'Unione europea, art. 16; cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 10; cfr. L. A. BYGRAVE, *EU Data Protection Law*, Wolters Kluwer, 2002, pag. 37.

⁷² V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, considerando 4.

⁷³ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, artt. 24, 25 e 32 e considerando 74 e 75; cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di),

prospettiva, il GDPR introduce parametri di legittimità sostanziale del trattamento espressi tramite i principi di liceità, correttezza, trasparenza, limitazione della finalità e minimizzazione dei dati, i quali devono orientare l'intera attività di trattamento⁷⁴. Tali principi si inseriscono in un quadro in cui, come affermato dalla Corte di giustizia già da prima dell'entrata in vigore del GDPR, ogni limitazione al diritto alla protezione dei dati deve rispettare i requisiti di necessità e proporzionalità⁷⁵.

Con specifico riferimento al tema in esame, la qualificazione del dato trattato come dato biometrico è cruciale. L'articolo 4, n. 14 del GDPR definisce i "dati biometrici" come dati personali ottenuti da un trattamento tecnico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona che ne consentono l'identificazione univoca⁷⁶. Tale disposizione va letta in combinato disposto con il Considerando 51 che precisa che le fotografie non costituiscano di per sé dati biometrici, ma che diventano tali se trattate con mezzi tecnici che permettano l'identificazione univoca dell'interessato, per cui i sistemi di riconoscimento facciale rientrano in tale definizione⁷⁷.

L'articolo 9, paragrafo 1 include i dati biometrici trattati per identificare in modo univoco una persona fisica tra le categorie peculiari di dati il cui trattamento, in linea di principio, è vietato⁷⁸: si tratta di dati particolarmente sensibili e idonei a incidere

La protezione dei dati personali in Italia, Zanichelli editore, 2019, pag. 17 s.; cfr. F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento. Una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in MediaLaws (www.medialaws.eu), pag. 107 ss.

⁷⁴ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 5

⁷⁵ Si veda Corte di Giustizia, Grande Sezione, sent. 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e. e. Kärntner Landesregierung e a.*, in Eur-Lex; Corte di Giustizia, Grande Sezione, sent. 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e a.*, in Eur-Lex, ove la Corte ha escluso la compatibilità con il diritto dell'Unione di una conservazione generalizzata e indiscriminata dei dati relativi alle comunicazioni elettroniche.

⁷⁶ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 4, n. 14

⁷⁷ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, considerando 51

⁷⁸ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 9, par. 1

significativamente sui diritti e le libertà fondamentali, quindi, l'utilizzo dei sistemi di riconoscimento facciale presuppone la ricorrenza di una delle deroghe previste dall'articolo 9, paragrafo 2, come il consenso esplicito o rilevanti motivi di pubblico interesse⁷⁹.

Tuttavia, la verifica di liceità del trattamento non si esaurisce nell'articolo 9. Il GDPR prevede infatti un duplice livello di tutela: anche quando ricorra una delle deroghe previste per le categorie particolari di dati, il trattamento deve comunque fondarsi su una delle basi giuridiche di cui all'articolo 6, quali, a seconda dei casi, il consenso dell'interessato, l'adempimento di un obbligo legale, la salvaguardia di interessi vitali o l'esecuzione di un compito di pubblico interesse⁸⁰. Quando il trattamento si fonda sul consenso, questo a fini di validità deve essere libero, specifico, informato e inequivocabile, secondo precisato dai considerando 42 e 43 del Regolamento⁸¹.

Ulteriore punto critico riguarda le decisioni basate solo sul trattamento automatizzato, inclusa la profilazione: tale argomento viene affrontato all'articolo 22 del GDPR. La disposizione afferma il diritto dell'interessato di non essere sottoposto a una decisione che si fondi unicamente sul trattamento automatizzato e che produca effetti giuridici che lo riguardino o che incida significativamente sulla sua persona. In questi casi, il Regolamento impone garanzie rafforzate tra cui il diritto a ottenere l'intervento umano, a esprimere la propria opinione e a contestare la decisione, anche al fine di prevenire rischi di discriminazione⁸².

Le garanzie individuali previste dal GDPR si collocano in una sistematica preventiva del rischio che è alla base di tutto il Regolamento. La potenziale incidenza dei sistemi

⁷⁹ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 9, par. 2

⁸⁰ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 6; cfr. F. BRAVO, *Le condizioni di liceità di trattamento dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 113 s.

⁸¹ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, considerando 42 e 43

⁸² V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 22

di riconoscimento facciale sui diritti fondamentali rende il trattamento qualificabile come “di rischio elevato”, ne consegue che l’impiego di questi sistemi su larga scala o in spazi pubblici può integrare i presupposti applicativi dell’articolo 35 del GDPR, che impone lo svolgimento di una valutazione di impatto sulla protezione dei dati, ovvero di uno strumento che valuta in anticipo la necessità e la proporzionalità del trattamento e i relativi rischi per i diritti fondamentali degli interessati⁸³.

Nel sistema delineato dal GDPR, accanto ai principi di liceità, proporzionalità e minimizzazione, e agli strumenti di valutazione preventiva del rischio, assume rilievo anche la figura del Data Protection Officer – cd DPO – disciplinata agli articoli 37, 38 e 39 del Regolamento. Tale figura si inserisce nella logica di accountability che permea dall’intero impianto del GDPR, in quanto mira a rafforzare dal punto di vista organizzativo la capacità del titolare del trattamento di conformare la propria attività alle prescrizioni europee in materia di protezione dei dati personali. La previsione del DPO, infatti, non risponde a una logica meramente formale, ma si collega all’esigenza di introdurre all’interno delle organizzazioni un presidio stabile di competenza, consulenza e sorveglianza che è particolarmente significativo in quei contesti in cui il trattamento presenta un’incidenza più intensa sui diritti e le libertà fondamentali degli interessati⁸⁴.

La designazione del DPO è prevista, in particolare, nei casi in cui il trattamento sia effettuato da un’autorità pubblica o da un organismo pubblico, nonché quando le attività principali del titolare o del responsabile consistano in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, oppure nel trattamento su larga scala di categorie particolari di dati personali quali sono i dati biometrici trattati per identificare in modo univoco una persona fisica. Proprio queste ragioni consentono al DPO di assumere una rilevanza particolare

⁸³ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 35 e considerando 75 e 91

⁸⁴ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 37, 38, 39; cfr. WP29, *Guidelines on Data Protection Officers*, WP243 rev.01, adottate il 13 dicembre 2016 ed emendate e adottate il 5 aprile 2017, pag. 5 s.; cfr. G. FINOCCHIARO, *Il quadro d’insieme sul regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 17 ss.

rispetto ai sistemi di riconoscimento facciale, in quanto essi, di regola, implicano trattamenti connotati da un'elevata complessità tecnica e un rischio significativo per i diritti fondamentali, specie se impiegati in contesti di monitoraggio sistematico o di identificazione biometrica⁸⁵.

Quanto alle sue funzioni, il DPO svolge compiti che possono essere ricondotti a tre principali linee direttrici: consulenza, sorveglianza e cooperazione con l'autorità di controllo. Sotto il primo profilo, esso informa e assiste il titolare del trattamento, il responsabile e i soggetti autorizzati circa gli obblighi derivanti dalla normativa europea e nazionale in materia di protezione dei dati personali. Sotto il secondo profilo, invece, il DPO vigila sull'osservanza del GDPR, delle politiche interne adottate dall'organizzazione in cui lavora e della corretta attribuzione delle relative responsabilità. Da ultimo, il DPO contribuisce anche alla diffusione, all'interno dell'organizzazione, di una più ampia cultura della protezione dei dati personali, svolgendo un'opera di sensibilizzazione e orientamento che assume particolare importanza nei contesti in cui la tecnologia può incidere in modo penetrante sulla posizione giuridica degli interessati⁸⁶.

Come chiarito dalle linee guida del Gruppo di lavoro Articolo 29, il DPO, tuttavia, non è il soggetto su cui ricade la responsabilità diretta per l'eventuale violazione del Regolamento, in quanto questa resta in capo al titolare o al responsabile del trattamento. Il DPO, piuttosto, svolge una funzione di presidio interno e di accompagnamento alla conformità⁸⁷.

⁸⁵ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 37, par. 1; cfr. WP29, *Guidelines on Data Protection Officers*, WP243 rev.01, adottate il 13 dicembre 2016 ed emendate e adottate il 5 aprile 2017, pag. 7; v. Garante privacy, *FAQ sul responsabile della protezione dei dati (RPD) in ambito pubblico*, nello specifico, FAQ su autorità/organismo pubblico

⁸⁶ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 39; cfr. WP29, *Guidelines on Data Protection Officers*, WP243 rev.01, adottate il 13 dicembre 2016 ed emendate e adottate il 5 aprile 2017, pag. 22 S., 33; cfr. A. AVITABILE, *Il responsabile della protezione dei dati*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 373 ss.

⁸⁷ Cfr. WP29, *Guidelines on Data Protection Officers*, WP243 rev.01, adottate il 13 dicembre 2016 ed emendate e adottate il 5 aprile 2017, pag. 5 s., 23, 33 s.

Il suo ruolo acquista un significato ancor più marcato nei trattamenti ad alto rischio, come quelli che coinvolgono tecnologie biometriche e di riconoscimento facciale. In questi casi, infatti, il DPO è chiamato a partecipare alle procedure di valutazione di impatto sulla protezione dei dati di cui all'articolo 35 del GDPR, contribuendo all'individuazione preventiva dei rischi che il trattamento può determinare per i diritti e le libertà fondamentali degli interessati, nonché delle misure idonee a mitigarli. Sotto questo profilo, la sua presenza assume una funzione propriamente preventiva in quanto consente l'emersione di eventuali criticità già nella fase di progettazione e implementazione del sistema, in coerenza con i principi di protezione dei dati by design e by default. Nel contesto dei sistemi di riconoscimento facciale, ciò implica che il DPO possa concorrere a valutare già in sede organizzativa non solo la liceità del trattamento dei dati biometrici, ma anche l'adeguatezza delle misure tecnico-organizzative, la proporzionalità dell'impiego della tecnologia e l'impatto che essa può avere sulle libertà personali⁸⁸.

Ulteriore elemento qualificante della figura è rappresentato dalle garanzie di indipendenza di cui all'articolo 38 del GDPR. Il Regolamento, infatti, stabilisce che il DPO non possa ricevere istruzioni per quanto riguarda l'esecuzione dei propri compiti, né essere rimosso o penalizzato dal titolare o dal responsabile del trattamento per l'adempimento delle sue funzioni. Queste garanzie mirano ad assicurare che la sua attività possa svolgersi con autonomia e imparzialità, evitando che la funzione di controllo interno venga svuotata da pressioni organizzative o da conflitti di interesse⁸⁹. Ne deriva che il DPO, pur non sostituendosi né al titolare del trattamento né all'autorità di controllo, costituisce un presidio interno di garanzia particolarmente rilevante nei

⁸⁸ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 35; cfr. WP29, *Guidelines on Data Protection Officers*, WP243 rev.01, adottate il 13 dicembre 2016 ed emendate e adottate il 5 aprile 2017, pag. 22 s., 33 s.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 181.

⁸⁹ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 38; cfr. WP29, *Guidelines on Data Protection Officers*, WP243 rev.01, adottate il 13 dicembre 2016 ed emendate e adottate il 5 aprile 2017, pag. 19 s., 33; v. Corte di giustizia, Sesta sezione, sent. 9 febbraio 2023, C-453/21, *X-FAB Dresden GmbH & Co. KG c. FC*.

trattamenti che presentano un potenziale lesivo elevato, come appunto quelli fondati sull'impiego di dati biometrici e tecniche di riconoscimento facciale⁹⁰.

Alla luce di ciò, il DPO può essere configurato come una figura centrale nel sistema di governance della protezione dei dati costruito dal GDPR. La sua funzione si colloca in un modello multilivello di tutela in cui la responsabilità primaria del rispetto della normativa grava sul titolare del trattamento, mentre le autorità indipendenti esercitano un controllo esterno. Tra questi due poli, il DPO opera come strumento di verifica, raccordo e prevenzione interno all'organizzazione, contribuendo a orientare le scelte tecniche e organizzative verso soluzioni compatibili con i principi europei sui dati personali. Proprio nei contesti in cui il trattamento dei dati si intreccia con tecnologie invasive e ad alto rischio, come nel caso del riconoscimento facciale, il suo coinvolgimento permette di rafforzare in concreto quella dimensione preventiva di tutela che costituisce uno dei pilastri del GDPR⁹¹.

Ciò non toglie, tuttavia, che i sistemi di riconoscimento facciale, proprio per la loro complessità tecnica e per la pluralità dei rischi che pongono, eccedano in parte il perimetro della sola disciplina in materia di protezione dei dati personali.

1.2 *Requisiti e obblighi per i sistemi di intelligenza artificiale alla luce dell'AI Act*

Sebbene il GDPR apra garanzie fondamentali in relazione al trattamento dei dati biometrici e introduca strumenti preventivi particolarmente significativi, esso non disciplina in modo espresso e compiuto i profili concernenti la progettazione, l'immissione sul mercato, l'affidabilità tecnica, la sicurezza e l'utilizzo dei sistemi di intelligenza artificiale in quanto tali.⁹² In questo quadro si colloca il Regolamento (UE) 2024/1689 – cd AI Act – che risulta essere complementare rispetto al GDPR, e

⁹⁰ Cfr. WP29, *Guidelines on Data Protection Officers*, WP243 rev.01, adottate il 13 dicembre 2016 ed emendate e adottate il 5 aprile 2017, pag. 19 s., 22 s., 33 s.; cfr. A. AVITABILE, *Il responsabile della protezione dei dati*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 373 ss.

⁹¹ Cfr. WP29, *Guidelines on Data Protection Officers*, WP243 rev.01, adottate il 13 dicembre 2016 ed emendate e adottate il 5 aprile 2017, pag. 22 s., 33 s.; v. art. 35 Reg. (UE) 2016/679

⁹² Cfr. EDPB-EDPS, *Joint Opinion 5/2021 for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, pag. 8 ss.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 320; cfr. A. MANTELERO, *Artificial intelligence, dati e diritti: spunti di riflessione per i regolatori*, in P. Bertoli, F. Ferrari, G. Ripamonti, G. Tiberi (a cura di), *Data protection tra Unione europea, Italia e Svizzera*, 2019, pag. 25 s.

segna un passaggio ulteriore nella costruzione di un quadro normativo europeo volto a disciplinare i sistemi di intelligenza artificiale non solo dal punto di vista del trattamento dei dati personali, ma anche sotto il profilo della loro progettazione, commercializzazione e impiego⁹³.

Obiettivo proclamato del Regolamento è migliorare il funzionamento del mercato interno promuovendo un'intelligenza artificiale affidabile, antropocentrica e rispettosa dei valori e dei principi fondamentali dell'Unione Europea⁹⁴.

A differenza del GDPR, che parte dal dato personale e dalla posizione giuridica dell'interessato, l'AI Act prende come punto di partenza il sistema tecnologico e ne disciplina tutto il ciclo vitale. La tecnica normativa impiegata è la classificazione dei sistemi per livello di rischio, e conseguente impianto regolatorio proporzionato, distinguendo:

- a- Pratiche vietate;
- b- Sistemi ad alto rischio;
- c- Sistemi soggetti a obblighi di trasparenza;
- d- Sistemi a rischio minimo⁹⁵.

In questo contesto i sistemi di identificazione biometrica remota – come il riconoscimento facciale – hanno un rilievo fondamentale. L'AI Act, in linea di principio, vieta l'uso a fini di law enforcement di sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico, salvo eccezioni tassative soggette a condizioni particolarmente rigorose. La ratio di questo divieto risiede nel rischio di sorveglianza generalizzata e indiscriminata, idonea a incidere sia sulla vita

⁹³ V. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*, art. 1; cfr. Commissione europea, aprile 2021, COM (2021) 206 final, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione*, in eur-lex (www.eur-lex.europa.eu), considerando 5, 6, ma anche il considerando 1 ss. del Regolamento (UE) 2024/1689

⁹⁴ V. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*, art. 1

⁹⁵ V. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*, art. 5

privata sia sulla protezione dei dati personali, nonché sulla libertà di circolazione, di riunione e sul principio democratico in generale⁹⁶.

Nelle poche eccezioni in cui tali sistemi si possono impiegare, i sistemi di identificazione biometrica rientrano, dal punto di vista regolamentare, nei sistemi ad alto rischio⁹⁷. Per questi ultimi il Regolamento impone un insieme particolarmente rigoroso di obblighi: l'istituzione di un sistema di gestione del rischio lungo l'intero ciclo di vita, requisiti di qualità e governance dei dati, predisposizione di una documentazione tecnica dettagliata, tracciabilità mediante registrazione automatica dei log, garanzie di trasparenza e informazione, nonché adeguata supervisione umana. In sostanza, il Regolamento in esame introduce una regolazione oggettiva delle tecnologie che vuole prevenire rischi sistemici, bias discriminatori ed errori incompatibili con i valori fondanti l'Unione Europea⁹⁸.

L'analisi congiunta del Regolamento (UE) 2016/679 e del Regolamento (UE) 2024/1689 evidenzia l'emersione nel diritto eurounitario di un modello regolatorio multilivello che ha lo scopo di regolare l'impatto delle tecnologie di riconoscimento facciale tramite strumenti al contempo complementari e diversi⁹⁹. Il GDPR ha come fulcro della disciplina la posizione dell'interessato e il controllo sul trattamento dei dati personali, quindi, alla base ha una logica prevalentemente soggettiva. L'AI Act, invece, rientra in una logica oggettiva e sistemica in quanto non si limita a valutare la legittimità del trattamento dei dati, ma interviene sulla conformazione del sistema tecnologico e ne disciplina l'intera vita in base a una graduatoria di rischio¹⁰⁰.

⁹⁶ Cfr. EDPB-EDPS, Joint Opinion 5/2021 *for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, pag. 2 s., 12; cfr. FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 24

⁹⁷ V. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*, art. 6, par. 2 in combinato disposto con l'allegato III, punto 1, lett. a), artt. da 9 a 15; cfr. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, adottato il 26 aprile 2023, pag. 7, 34, 38

⁹⁸ V. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*, artt. da 9 a 15; cfr. EDPB-EDPS, Joint Opinion 5/2021 *for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, pag. 9 s.

⁹⁹ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 135

¹⁰⁰ V. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*, artt. 1, 5 e 9

I sistemi di riconoscimento facciale rappresentano l'intersezione paradigmatica di tali logiche e impongono un'interpretazione coordinata delle fonti. In tale contesto normativo multilivello assumono un ruolo centrale anche le autorità indipendenti di protezione dei dati, chiamate a garantire l'applicazione concreta delle garanzie previste dal diritto europeo¹⁰¹.

2. *Le autorità di controllo nel sistema europeo di protezione dei dati*

Accanto al quadro normativo delineato dal GDPR e più recentemente dall'AI Act, assume un ruolo centrale la dimensione istituzionale della protezione dei dati personali e, in particolare, dei dati biometrici.

Parte della dottrina evidenzia come il dato biometrico – in quanto informazione che consente l'identificazione univoca di una persona fisica e derivante da un trattamento tecnico specifico – imponga tutele rafforzate e condizioni di liceità più severe rispetto al trattamento di altri dati personali, nonché particolari cautele nella valutazione d'impatto sui diritti fondamentali¹⁰².

Il sistema creato con il GDPR prevede un'architettura istituzionale multilivello volta a garantire un'applicazione coerente e uniforme della disciplina in tutta l'Unione Europea¹⁰³: tale modello mira a superare la frammentazione nazionale, che era propria della Direttiva 95/46/CE¹⁰⁴, configurando un sistema integrato di cooperazione e coerenza¹⁰⁵.

¹⁰¹ Cfr. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, adottato il 26 aprile 2023, pag. 7.

¹⁰² Cfr. A. CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 208 s.; cfr. F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo Regolamento: una sfida per le autorità di controllo e una difesa per la libertà dei moderni*, in MediaLaws (www.medialaws.eu), pag. 106, 109 s.

¹⁰³ Cfr. M. S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra le autorità garanti*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 707 ss.

¹⁰⁴ Cfr. Dir. 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*.

La scelta dello strumento della direttiva, anziché del regolamento, rifletteva la fase ancora iniziale del processo di armonizzazione europea in materia di protezione dei dati personali, lasciando agli Stati membri un margine di adattamento nell'attuazione degli obiettivi comuni.

¹⁰⁵ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 68.

In questo quadro, il Garante europeo per la protezione dei dati – European Data Protection Supervisor o EDPS – svolge un ruolo essenziale quale autorità indipendente incaricata di vigilare sul trattamento dei dati personali effettuato dalle istituzioni e dagli organismi dell’Unione europea, nonché di fornire consulenza sulle politiche e sugli atti normativi dell’Unione che incidono sulla protezione dei dati personali¹⁰⁶. L’autorità – anche in accordo con le autorità nazionali e il Comitato europeo – ha posto attenzione ai rischi intrinseci delle tecnologie biometriche, evidenziando come l’uso di sistemi come il riconoscimento facciale in spazi pubblicamente accessibili possa compromettere l’anonimato nelle aree pubbliche e interferire con le libertà fondamentali. In questa prospettiva, l’Autorità ha sostenuto un approccio fortemente improntato alla prevenzione del rischio, fondato sull’idea che, in presenza di tecnologie potenzialmente lesive dei diritti fondamentali, debbano essere adottate cautele rigorose anche quando non vi sia ancora una certezza scientifica assoluta circa la portata del danno¹⁰⁷.

Parallelamente, il Comitato europeo per la protezione dei dati¹⁰⁸ – European Data Protection Board o EDPB – coordina le autorità di controllo nazionali e assicura un’applicazione coerente del Regolamento in tutta l’Unione Europea anche mediante linee guida e pareri su questioni transfrontaliere.

In materia di riconoscimento facciale, l’EDPB ha adottato le Linee guida 05/2022 sull’uso della tecnologia di riconoscimento facciale¹⁰⁹ che forniscono indicazioni interpretative su come conciliare l’impiego di tali sistemi con i principi di necessità, proporzionalità e rispetto dei diritti fondamentali, richiamando anche la Direttiva 2016/680 (Direttiva Polizia)¹¹⁰ in combinato disposto con il GDPR. Inoltre, nel 2024

¹⁰⁶ V. Reg. (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, *relativo alla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell’Unione e sulla libera circolazione di tali dati*, artt. 52, parr. 2 e 3

¹⁰⁷ Cfr. EDPB-EDPS, *Joint Opinion 05/2021 on the proposal for a regulation laying down harmonized rules on artificial intelligence (AI Act)*, pag. 2 s.; cfr. EDPB-EDPS, *Call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination*, Giugno 2021, pag. 2

¹⁰⁸ Istituito dall’articolo 68 del GDPR

¹⁰⁹ V. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, adottato il 26 aprile 2023, pag. 23, 42

¹¹⁰ Insieme al GDPR formano il “Pacchetto europeo per la protezione dei dati personali”. La Direttiva disciplina in modo specifico il trattamento dei dati personali da parte degli organi di polizia e delle autorità giudiziarie per finalità di indagine e di sanzioni penali.

il Comitato ha adottato un parere specifico sull'uso del riconoscimento facciale negli aeroporti per regolare l'uso dei dati biometrici ai fini dell'efficientamento del flusso di passeggeri. In tale atto, l'EDPB ha sottolineato l'importanza del controllo individuale dei dati e la conformità ai principi del GDPR, in particolare quelli relativi alla limitazione della conservazione, alla sicurezza del trattamento e alla protezione dei dati by design e by default – quindi, durante tutto il ciclo di vita del sistema¹¹¹.

La dottrina ha sottolineato come tali strumenti interpretativi dell'EDPB siano essenziali per la comprensione applicativa delle norme di cui al GDPR in scenari tecnologici complessi, segnando un'evoluzione dell'approccio regolatorio europeo: si passa dalla mera interpretazione normativa a una governance attiva delle tecnologie emergenti, con riferimento particolare al bilanciamento tra innovazione e tutela dei diritti fondamentali¹¹².

L'interazione tra il Comitato europeo per la protezione dei dati e il Garante europeo per la protezione dei dati, inoltre, evidenzia come la governance europea sia strutturata su un modello duale: vigilanza e consulenza sulle istituzioni dell'UE tramite l'EDPS e armonizzazione dell'applicazione del GDPR tra gli Stati membri tramite l'EDPB¹¹³. Questa architettura istituzionale consente di coniugare innovazione tecnologica e tutela dei diritti fondamentali, imponendo soprattutto nei contesti di riconoscimento facciale, un approccio preventivo basato sulla valutazione d'impatto, sulla responsabilizzazione dei titolari del trattamento e sul controllo indipendente delle autorità competenti¹¹⁴.

V. Dir. (UE) 2016/680 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati*

¹¹¹ V. European Data Protection Board, *Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow*, pag. 36 s.

¹¹² Cfr. F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le autorità di controllo e una difesa per la libertà dei moderni*, pag. 107 ss.

¹¹³ V. Reg. (UE) 2018/1725 del Parlamento europeo e del Consiglio, 23 ottobre 2018, *relativo alla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati*; v. art. 68 del Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*

¹¹⁴ Cfr. EDPB, *Guidelines 05/2022, on the use of facial recognition technology in the area of law enforcement*, version 2.0, adottato il 26 aprile 2023, pag. 7, 34 ss.; cfr. Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, *relativo alla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi*

Nel settore del riconoscimento facciale, il rilievo dell'EDPS e dell'EDPB risiede soprattutto nella loro capacità di trasformare principi generali in criteri applicativi concreti. Attraverso pareri, linee guida e attività di coordinamento, tali organismi contribuiscono a delimitare l'impiego delle tecnologie biometriche entro parametri di necessità, proporzionalità e controllo effettivo. La dimensione istituzionale assume così una funzione di stabilizzazione del quadro europeo, rendendo più prevedibile l'applicazione delle garanzie anche nei contesti tecnologicamente più complessi.

3. Italia: dal Codice privacy alla legge 132/2025

Accanto al quadro normativo europeo, anche l'ordinamento italiano ha progressivamente sviluppato strumenti giuridici volti a disciplinare l'impiego delle tecnologie digitali e, in particolare, delle applicazioni basate sull'intelligenza artificiale¹¹⁵.

Nel diritto interno, la regolazione dell'uso di tecnologie riconducibili al riconoscimento facciale è stata costruita per stratificazione: dapprima tramite la disciplina generale del trattamento dei dati personali, poi mediante atti di indirizzo e prescrizioni in materia di biometria e da ultimo tramite una cornice legislativa in tema di intelligenza artificiale¹¹⁶.

Il decreto legislativo n. 196/2003 – recante il Codice in materia di protezione dei dati personali o Codice privacy – rappresenta la prima architettura organica italiana in materia di protezione dei dati personali. Esso nasce in attuazione della direttiva 95/46/CE e segna un passaggio fondamentale nell'evoluzione della tutela della persona nell'ordinamento italiano, sistematizzando in un unico testo normativo una disciplina che, fino a quel momento, risultava frammentaria¹¹⁷.

dell'Unione e sulla libera circolazione di tali dati, e Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*

¹¹⁵ V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), art. 1; cfr. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Zanichelli editore, novembre 2025, pag. 169 ss.

¹¹⁶ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 122, 136, 240 ss.; cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale* (www.sistemapenale.it), fascicolo 9/2022, pag. 37 s.

¹¹⁷ V. d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), art. 1; cfr. G. FINOCCHIARO, *Diritto di Internet*, Zanichelli editore, 2023, pag. 21 s.; cfr. S. RODOTÀ, *Tecnologie e diritti*, Il mulino, 2021, pag. 46 s.

Anche dopo l'entrata in vigore del GDPR, che ha comportato un significativo intervento mediante il decreto legislativo n. 101/2018, il Codice continua a costituire il punto di riferimento interno per la regolazione del trattamento dei dati personali, in particolare nei settori in cui il legislatore nazionale conserva dei margini di intervento. Esso opera oggi come la normativa di raccordo all'interno di un sistema multilivello in cui la protezione dei dati personali è riconosciuta come diritto fondamentale¹¹⁸.

Il punto di partenza del Codice privacy è il riconoscimento della protezione dei dati quale espressione della dignità della persona e presidio delle libertà fondamentali. Non si tratta più soltanto di tutela della riservatezza in senso statico, ma di protezione del controllo dell'individuo sulle informazioni che lo riguardano, in una dimensione dinamica e relazionale¹¹⁹. Il trattamento dei dati deve avvenire nel rispetto dei principi di liceità, correttezza, necessità, proporzionalità e minimizzazione, che costituiscono l'ossatura garantistica del sistema¹²⁰.

In questo quadro si inseriscono anche le tecnologie di riconoscimento facciale. Sebbene non ne troviamo una menzione espressa nel Codice, tali sistemi rientrano nella nozione di trattamento di dati biometrici e poiché sono difficilmente modificabili, il loro trattamento comporta un livello di rischio superiore rispetto a quello di altri dati personali e ciò rende centrale l'applicazione rigorosa dei principi di necessità e proporzionalità¹²¹. In questa prospettiva, il Codice offre una disciplina indiretta del

¹¹⁸ V. d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), artt. 2-ter e 2-septies; cfr. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli, 2019, pag. 5; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 135

¹¹⁹ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 35; v. d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), art. 2-quinquiesdecies; cfr. G. FINOCCHIARO, *Diritto di Internet*, Zanichelli editore, 2023, pag. 20; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 77

¹²⁰ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 158, 167 ss.; cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale* (www.sistemapenale.it), fascicolo 9/2022, pag. 3; cfr. A. MANTELEO, *Artificial Intelligence, dati e diritti: spunti di riflessione per i regolatori*, in P. Bertoli, F. Ferrari, G. Ripamonti, G. Tiberi (a cura di) *Data protection tra Unione europea, Italia e Svizzera*, 2019, pag. 24 s.

¹²¹ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 136, 158; cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale*, fascicolo 9/2022, pag. 24 s.

riconoscimento facciale: la legittimità del trattamento dipende dalla presenza di una base giuridica adeguata, dal rispetto del principio di minimizzazione, dalla limitazione della finalità e dall'adozione di opportune misure di sicurezza¹²². Inoltre, nei casi in cui il trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche, è prevista la necessità della valutazione di impatto sulla protezione dei dati (c.d. DPIA), che costituisce uno strumento di prevenzione e responsabilizzazione del titolare¹²³.

Sotto questo profilo, il Codice – soprattutto se letto in combinazione con il GDPR – dimostra una notevole capacità adattiva: pur essendo stato concepito in un'epoca precedente alla diffusione massiva delle tecnologie biometriche e dei sistemi di intelligenza artificiale, la sua struttura per principi consente di ricondurre anche fenomeni tecnologicamente complessi entro un quadro di tutela giuridica coerente. Tuttavia, proprio questa impostazione generale evidenzia alcuni limiti strutturali se applicata a tecnologie ad alta intensità invasiva come il riconoscimento facciale¹²⁴.

Una prima lacuna risiede nell'assenza di una tipizzazione normativa autonoma del riconoscimento facciale e di un distinguo espresso delle diverse modalità tecniche e funzionali di tali sistemi. Ne deriva che la qualificazione giuridica avviene ex post ad opera dei giudici o delle amministrazioni e viene fatta tramite sussunzione, ovvero facendole rientrare in categorie generali¹²⁵. Ciò provoca incertezza perché c'è oscillazione applicativa: la stessa tecnologia può essere trattata come strumento di autenticazione o come meccanismo di sorveglianza a seconda del contesto in cui opera. Questa lacuna impedisce di instaurare nell'ordinamento un sistema garantista e

¹²² Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 144, 158, 167, 172; cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale*, fascicolo 9/2022, pag. 24 s.

¹²³ V. d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), articoli 2-ter, 2-septies e 2-quinquiesdecies; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 129

¹²⁴ Sebbene venga usato il termine lacune, non significa che l'ordinamento è sprovvisto di tutela, infatti molte disposizioni mirano a bloccare o sanzionare queste pratiche.

Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 119 ss., 287

¹²⁵ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 119 ss., 136; cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale* (www.sistemapenale.it), fascicolo 9/2022, pag. 37 s.

calibrato sulle specificità del riconoscimento facciale, la cui pericolosità risiede nella sua capacità di identificazione diffusa nello spazio sociale¹²⁶.

Una seconda lacuna riguarda la scarsa differenziazione normativa per contesto: le norme sono applicabili sia al privato che al pubblico, ma non creano un regime interno chiaro che distingua, ad esempio, l'uso commerciale dall'uso lavoristico, o l'uso in spazi pubblici per scopi di sicurezza dall'uso investigativo. Ciò produce un paradosso in quanto, tanto più l'uso è sensibile in termini di ampiezza del pubblico coinvolto o di incidenza sulle libertà, tanto più diventa cruciale una base legale determinata e relative procedure rafforzate¹²⁷. Nel contesto pubblico e di sicurezza la dottrina parla di "lacuna regolatoria qualificata", per cui non una mera assenza di dettaglio, ma un deficit ex ante di una tecnologia che potenzialmente può incidere sulle libertà fondamentali¹²⁸.

Terzo profilo riguarda l'asimmetria tra le tutele reattive e quelle preventive. In Italia la protezione contro gli usi sproporzionati del riconoscimento facciale si realizza tramite strumenti successivi o correttivi o tramite obblighi di valutazione preventiva dei rischi e ciò non equivale a un regime autorizzatorio espresso e delineato anche per quelle applicazioni più invasive. Quindi, la conformità può dipendere da quello che è il sistema di controllo e dalla qualità delle valutazioni effettuate dai titolari del trattamento, ma non da regole legislative previe¹²⁹.

¹²⁶ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 11 ss., 95; cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale* (www.sistemapenale.it), fascicolo 9/2022, pag. 23 ss.

¹²⁷ V. d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), artt. 2-ter, 2-septies e 2-quinquiesdecies; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 158; cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale*, fascicolo 9/2022, pag. 27

¹²⁸ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 119, 158, 287; cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale*, fascicolo 9/2022, pag. 27, 37

¹²⁹ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 35; v. d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), art. 2-quinquiesdecies; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 129, 158, 244; cfr. A. MANTELERO, *Artificial Intelligence, dati e diritti: spunti di riflessione per i regolatori*, in P. Bertoli, F.

Infine, un'ultima lacuna riguarda la governance dell'interoperabilità e del function creep: se non vengono istituiti dei limiti normativi, un sistema che viene creato per una finalità, progressivamente può essere integrato con altri sistemi tecnologici trasformandosi in uno strumento di identificazione diffusa o di profilazione. Il diritto positivo offre dei limiti nei fini e impone il rispetto della necessità e della proporzionalità, ma non offre – ancora – un set di barriere tecniche e giuridiche che impediscano l'espansione funzionale di tali sistemi. Tale rischio, peraltro, è particolarmente critico perché il salto da un uso circoscritto a uno generalizzato può avvenire in modo graduale e poco percepibile per l'interessato¹³⁰.

L'analisi del Codice privacy mostra, dunque, come la sua struttura per principi continui a offrire un presidio fondamentale, ma al tempo stesso non consenta, da solo, di regolare in modo puntuale le applicazioni biometriche più invasive.

Il Codice privacy consente di ricondurre il riconoscimento facciale nella cornice del trattamento dei dati biometrici, ma la legge 132/2025, che si inserisce nel quadro regolatorio delineato dall'AI Act, segna un passaggio ulteriore in quanto non si limita a disciplinare l'informazione personale, ma interviene anche sulla dimensione tecnologica dei sistemi di intelligenza artificiale. Il rapporto tra le due normative, d'altro canto, evidenzia una tensione:

- La prima offre una tutela per principi applicabile ex ante ed ex post al trattamento dei dati personali¹³¹
- La seconda introduce una cornice più ampia, ma meno tipizzata e lascia aperta la questione della regolazione puntuale delle tecnologie biometriche ad alto impatto¹³².

Ferrari, G. Ripamonti, G. Tiberi (a cura di), *Data protection tra Unione europea, Italia e Svizzera del 2019*, pag. 26

¹³⁰ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 247, 275; cfr. A. MANTELERO, *Artificial Intelligence, dati e diritti: spunti di riflessione per i regolatori*, in P. Bertoli, F. Ferrari, G. Ripamonti, G. Tiberi (a cura di), *Data protection tra Unione europea, Italia e Svizzera del 2019*, pag. 24 s.

¹³¹ Si tratta di tutele preventive, ma non esiste una disciplina preventiva specifica e di dettaglio per le applicazioni più invasive del riconoscimento facciale.

¹³² V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), artt. 1, 3 e 24; cfr. F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le autorità di controllo e una difesa per la libertà dei moderni*, 116 s.; cfr. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Zanichelli editore, novembre 2025, pag. 181 ss.

La legge appena menzionata rappresenta il primo intervento organico del nostro ordinamento per definire una cornice nazionale sull'intelligenza artificiale, in un contesto in cui la disciplina europea resta il riferimento¹³³.

Anche tale intervento si configura come una legge-quadro: non costruisce un regime dettagliato per ogni tecnologia, ma enuncia principi generali e prevede discipline di settore e deleghe al Governo che vogliono promuovere la ricerca e l'innovazione in una dimensione antropocentrica, mantenendo però fermo il coordinamento con il regolamento (UE) 2024/1689¹³⁴.

L'impostazione della normativa in esame ruota intorno a due scelte di tecnica normativa:

- 1) Dispone un nucleo di principi generali che fungono da criteri interpretativi e da standard di legittimità per l'uso dell'IA nei vari ambiti applicativi.
- 2) Detta una serie di discipline di settore e una serie di deleghe al Governo per completare il quadro normativo, coordinandolo con la disciplina eurounitaria e i profili di enforcement¹³⁵.

Il nostro legislatore non va a sostituire il diritto europeo, ma tenta di declinare la sua logica nel contesto interno, soprattutto in punto di rilevanza delle garanzie pubblicistiche, procedimentali e di responsabilità. Appare emblematica, in tal senso, la norma dedicata all'uso dell'intelligenza artificiale nella Pubblica amministrazione che lega espressamente l'impiego di tali sistemi a fini di efficienza e qualità dei servizi, ma richiede anche la conoscibilità del funzionamento e la tracciabilità dell'utilizzo, oltre a ribadire la necessità di preservare la dimensione umana della decisione

¹³³ V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), art. 14, commi 1-2; cfr. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Zanichelli editore, novembre 2025, pag. 170 s. cfr. O. POLLICINO, G. MUTO, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, pag. 394 ss.

¹³⁴ V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), art. 3, co. 1-4; cfr. O. POLLICINO, G. MUTO, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, pag. 394 ss.; cfr. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Zanichelli editore, novembre 2025, pag. 172 s.

¹³⁵ V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), art. 3, co. 3 e 14, co. 1; cfr. O. POLLICINO, G. MUTO, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, pag. 394 ss.

amministrativa. Tale norma consolida la dottrina del non esclusivo affidamento all'algoritmo, restando la persona umana l'unica responsabile del procedimento e del provvedimento¹³⁶.

La legge 132/2025 non disciplina in modo diretto il riconoscimento facciale, né lo definisce o elenca usi consentiti e vietati, tuttavia ciò non significa che non sia una normativa rilevante per la materia. La sua incidenza è indiretta e al contempo strutturale perché molte applicazioni del riconoscimento facciale costituiscono modelli di intelligenza artificiale che sono potenzialmente idonei a incidere sui diritti e le libertà fondamentali¹³⁷. Sono quindi state sviluppate alcune linee direttrici fondamentali. Anzitutto, assume rilievo il principio di trasparenza e conoscibilità dell'uso dei sistemi di intelligenza artificiale: il riconoscimento facciale è una tecnologia che opera spesso in modo non percepibile dall'interessato e l'identificazione può avvenire a distanza tramite i sistemi di videosorveglianza integrati con gli algoritmi di comparazione biometrica per cui il soggetto può non essere consapevole del processo in atto. In tal senso la previsione della legge 132, in merito alla necessità di rendere conoscibile l'utilizzo dei sistemi di IA assume peculiare rilevanza anche per il riconoscimento facciale. La conoscibilità non riguarda solo l'esistenza del sistema, ma implica una trasparenza quantomeno funzionale sulle finalità perseguite, la seguente logica generale del funzionamento e il ruolo dell'intervento umano. Ciò andrebbe a ridurre il rischio di opacità decisionale che è una delle principali criticità delle tecnologie biometriche¹³⁸.

¹³⁶ Per un approfondimento si veda *dal procedimento digitale all'amministrazione algoritmica responsabile: la nuova disciplina dell'intelligenza artificiale nella pubblica amministrazione dopo la Legge n. 132/2025* in Amministrazione e Contabilità dello Stato e degli enti pubblici del 16 ottobre 2025.

V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), art. 14, commi 1-2; cfr. M. BASSINI, O. POLLICINO, *La Cassazione sul "consenso algoritmico". Ancora un tassello nella costruzione di uno statuto giuridico composito*, in Giustizia Insieme (www.giustiziainsieme.it), 21 giugno 2021, pag. 4

¹³⁷ V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), art. 3, co. 1-4; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 38, 57

¹³⁸ V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), art. 3, comma 3, e art. 14, co. 1; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 11, 184 ss., 209; cfr. M. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in Sistema penale (www.sistemapenale.it), fascicolo 9/2022, pag. 24 s., 30 s.

Un secondo profilo di raccordo concerne il principio di non discriminazione. Il dibattito scientifico ha evidenziato come i sistemi di riconoscimento facciale possano presentare margini di errore differenziati in base al gruppo demografico di riferimento che può comportare una potenziale lesione dell'eguaglianza sostanziale. La legge 132, nel richiamare espressamente la necessità di prevenire tali effetti discriminatori nell'uso dei sistemi di IA, rafforza la prospettiva per cui il problema del riconoscimento facciale non è esclusivamente legato alla protezione dei dati personali, ma investe più ampiamente la dimensione dell'eguaglianza e dell'equità delle decisioni automatizzate. In tal senso, l'incidenza della legge si estende alla valutazione della qualità tecnica dei modelli, alla verifica dei dataset usati e alla necessità di un monitoraggio costante del funzionamento del sistema¹³⁹.

Ultimo profilo di raccordo è rappresentato dal principio di supervisione umana e di tracciabilità: la legge 132 del 2025 ribadisce che i sistemi di IA devono operare come supporto e non in modo sostitutivo dell'attività decisoria umana. In applicazione ai sistemi di riconoscimento facciale, tale principio implica che l'identificazione automatica non può tradursi in una decisione automatizzata priva di una verifica critica: l'identificazione automatica deve essere accompagnata da un controllo umano, quindi da una valutazione del contesto ai fini di prevenire errori e/o abusi. Inoltre, la tracciabilità dell'utilizzo consente di ricostruire l'iter decisionale che è il fondamento di ogni successiva contestazione o controllo¹⁴⁰.

In questa chiave, la legge opera come un ponte che rafforza la lettura costituzionalmente orientata dell'utilizzo di tali tecnologie.

Nonostante tutto, proprio perché è stata costruita come una legge quadro, essa presenta delle lacune rilevanti se valutata rispetto ai sistemi di riconoscimento facciale. Ancora non è stata introdotta la distinzione delle tipologie di riconoscimento facciale, né tra l'uso ex post e in tempo reale, né tra impiego in spazi privati e pubblici; di

¹³⁹ V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), artt. 1, 3, 14 e 24; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 217 ss., 317 ss.; cfr. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Zanichelli editore, novembre 2025, pag. 174 ss.

¹⁴⁰ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 193, 209; cfr. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Zanichelli editore, novembre 2025, pag. 174 ss.

conseguenza la disciplina resta affidata alla combinazione di principi generali e fonti eurounitarie, ma permane il rischio che il bilanciamento tra l'innovazione e i diritti fondamentali sia compiuta “caso per caso” e non tramite criteri predeterminati normativamente¹⁴¹.

In secondo luogo, l'ampio ricorso alle deleghe consente una forma di adattabilità che però sposta in avanti molte scelte decisive per quanto riguarda le procedure, le competenze e i meccanismi di controllo. Da ciò deriva la possibilità di un vuoto operativo nel breve periodo in quanto la tutela concreta dipende da come e quando saranno adottati i decreti attuativi e da come verrà armonizzato il sistema delle autorità coinvolte¹⁴².

Da ultimo, la legge non chiude sul piano nazionale il problema delle applicazioni più invasive dei sistemi di riconoscimento facciale. In questi casi sarebbe da auspicare un livello elevato di prevedibilità ex ante e relative garanzie procedurali in quanto l'impatto potenziale non riguarda solo il diritto alla riservatezza, ma anche l'esercizio delle libertà costituzionali¹⁴³.

In conclusione, la legge 132/2025 segna un passaggio importante nella costruzione di un lessico nazionale dell'“IA responsabile”, rafforzando il raccordo tra innovazione e diritti fondamentali e offrendo criteri interpretativi utili anche per tecnologie non nominate espressamente, come il riconoscimento facciale. Al contempo, proprio rispetto a quest'ultimo, emerge un limite tipico delle leggi-quadro: la tutela è prevalentemente indiretta e di principio, mentre resta aperta la definizione delle regole operative e delle garanzie per le applicazioni biometriche ad alto rischio¹⁴⁴.

¹⁴¹ V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), artt. 1, 3, 14 e 24; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 119 ss., 158, 240

¹⁴² V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), art. 24; cfr. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Zanichelli editore, novembre 2025, pag. 181 ss.

¹⁴³ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 57, 95, 158; cfr. COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale* (www.sistemapenale.it), fascicolo 9/2022, pag. 27, 37

¹⁴⁴ V. l. 23 settembre 2025, n. 132 (Disposizioni e deleghe al Governo in materia di intelligenza artificiale), artt. 1, 3, 14 e 24; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 287, 320; cfr. G. FINOCCHIARO, *Diritto dell'intelligenza artificiale*, Zanichelli editore, novembre 2025, pag. 170, 181 ss.

Accanto alle fonti normative che compongono il quadro italiano in materia di protezione dei dati personali, assume rilievo anche il ruolo svolto dal Garante per la protezione dei dati personali, ovvero un'autorità amministrativa indipendente cui l'ordinamento affida il compito di vigilare sull'osservanza della disciplina relativa al trattamento dei dati. A tale Autorità spettano non solo poteri di controllo, correttivi e sanzionatori, ma anche funzioni consultive e di indirizzo, con cui concorre significativamente all'attuazione concreta delle garanzie predisposte dal legislatore nazionale ed europeo¹⁴⁵.

La centralità di tale figura nel sistema non dipende solo dalla possibilità di intervenire ex post sui trattamenti illeciti, ma anche dalla capacità di orientare in via preventiva l'interpretazione e l'applicazione della normativa in settori caratterizzati da particolari complessità e da un più elevato impatto sui diritti fondamentali. Proprio per questa ragione il suo ruolo ha assunto un rilievo crescente anche in riferimento alle tecnologie biometriche e, in particolare, ai sistemi di riconoscimento facciale, rispetto ai quali l'Autorità ha progressivamente contribuito a individuare limiti, presupposti e condizioni di liceità¹⁴⁶.

Nel complesso, il quadro italiano mostra una regolazione del riconoscimento facciale ancora non pienamente compiuta, in cui, accanto alle fonti legislative, un ruolo cruciale è stato ed è svolto proprio dall'attività interpretativa e applicativa del Garante privacy. Il Codice privacy continua a offrire il presidio fondamentale sul piano della protezione dei dati e della tutela della persona, mentre la legge 132/2025 introduce una cornice ulteriore di principi e di governance riferita ai sistemi di intelligenza artificiale. Proprio la natura generale e astratta di tali fonti consente, da un lato, di adattare la disciplina all'evoluzione tecnologica e di ricondurre entro una medesima cornice applicazioni anche molto diverse tra loro. Dall'altro lato, tuttavia, questa stessa

¹⁴⁵ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 58; v. d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) art. 154; cfr. E. GUARDIGLI, *Le autorità di controllo: dalla Direttiva 95/46/CE al Regolamento 679/2016*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, Zanichelli editore, 2019, pag. 686 ss.

¹⁴⁶ V. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, art. 58 parr. 1 e 2; cfr. V. PAGNANELLI, *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, in Osservatorio sulle fonti, n. 2/2021, pag. 800 ss.

impostazione mostra i suoi limiti quando venga in rilievo l'impiego delle tecnologie biometriche più invasive, rispetto alle quali il solo ricorso ai principi generali può non garantire un livello sufficiente di prevedibilità ex ante e di differenziazione delle garanzie. La criticità principale, pertanto, non risiede tanto nell'assenza di principi, quanto nella difficoltà di tradurli in regole più puntuali per i contesti nei quali il riconoscimento facciale incide sullo spazio pubblico e sull'esercizio delle libertà fondamentali.

4. Il Garante per la protezione dei dati personali e i sistemi di riconoscimento facciale – un'analisi per casi

L'elaborazione del pensiero del Garante in materia di riconoscimento facciale non si rinviene in un solo atto di indirizzo generale, bensì emerge progressivamente tramite i suoi pareri, i suoi provvedimenti e i suoi interventi sanzionatori¹⁴⁷ che consentono di ricostruire l'orientamento maturato rispetto all'impiego di tali tecnologie. La linea interpretativa si può ricostruire tramite tre casi emblematici: SARI Real Time, Clearview AI e le sperimentazioni del faceboarding in ambito aeroportuale¹⁴⁸.

4.1 Il caso SARI – tra l'investigazione e l'identificazione biometrica in tempo reale

Il sistema SARI – Sistema Automatico di Riconoscimento delle Immagini – è stato sviluppato nel 2017 dal Ministero dell'interno nell'ambito del processo di modernizzazione tecnologica delle attività di pubblica sicurezza e di supporto alle indagini delle forze dell'ordine. La sua introduzione si inserisce nel più ampio processo di digitalizzazione degli strumenti investigativi avviato negli ultimi anni dalle amministrazioni di pubblica sicurezza, volto a rafforzare le capacità di analisi delle immagini provenienti da sistemi di videosorveglianza e altre fonti digitali¹⁴⁹.

¹⁴⁷ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 240 ss.; V. A. FONSI, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in Penale. Diritto e Procedura (www.penaledp.it), n. 2/2021, pag. 289 s.

¹⁴⁸ V. rispettivamente Garante per la protezione dei dati personali, parere 25 marzo 2021, doc. web 9575877; ordinanza-ingiunzione 10 febbraio 2022, doc. web 9751362; provvedimento 11 settembre 2025, doc. web 10167745 in Garante Privacy (www.garanteprivacy.it)

¹⁴⁹ V. Garante privacy, provv. 25 marzo 2021, n. 127, doc. web n. 9575877; cfr. *Memoria del Presidente del Garante per la protezione dei dati personali*, prof. P. Stanzone, 7 febbraio 2024 nell'ambito dell'indagine conoscitiva sull'intelligenza artificiale, doc. web n. 9982816

SARI si articola in due modalità di funzionamento, che implicano un diverso grado di incidenza sui diritti fondamentali, ovvero:

- SARI Enterprise;
- SARI Real Time¹⁵⁰.

SARI Enterprise opera in modalità differita e consente di confrontare l'immagine di un soggetto, acquisita nel corso di un'attività investigativa, con le immagini presenti negli archivi segnaletici delle forze dell'ordine. In questa configurazione, il sistema non realizza una sorveglianza continua dello spazio pubblico, ma viene utilizzato ex post, a partire da un'immagine già acquisita nell'ambito di un'indagine. Tale caratteristica, tuttavia, non elimina ogni problematicità: la Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica ha confermato che il database usato da tale applicativo è esclusivamente quello della banca dati A.F.I.S. A maggio 2025 i soggetti profilati risultavano essere 2.759.520 cittadini italiani, 1.156.544 cittadini dell'Unione Europea e 13.975.872 cittadini extra-europei. Quanto al funzionamento concreto, il sistema non restituisce un'identificazione certa, ma una lista di candidati ordinati per grado di similarità, che deve essere sempre verificata manualmente da un operatore qualificato¹⁵¹. SARI Enterprise, quindi, non opera su un archivio neutro o comunque rappresentativo della popolazione generale, bensì su una banca dati alimentata da precedenti attività di identificazione e fotosegnalazioni. La significativa presenza di cittadini extra-europei nell'archivio si collega anche alla disciplina amministrativa dell'immigrazione che prevede specifiche ipotesi di sottoposizione dello straniero a rilievi fotodattiloscopici e segnaletici¹⁵². Il punto critico, dunque, non consiste nell'affermare che SARI Enterprise sia necessariamente utilizzato con finalità discriminatorie, ma nel rilevare come l'apparente neutralità del confronto biometrico

¹⁵⁰ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 245; cfr. G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuri sviluppi normativi sul fronte europolitano*, in *La Legislazione Penale* (www.lalegislazonepenale.eu), dicembre 2021, pag. 4 ss.

¹⁵¹ Cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica, una ricerca sul campo*, Giappichelli, 2026, pag. 192

¹⁵² Nello specifico, l'art. 5, comma 2-bis e 4-bis del Testo Unico sull'Immigrazione prevedono, rispettivamente, che lo straniero che richiede il permesso di soggiorno o il suo rinnovo sia sottoposto a rilievi fotodattiloscopici, inoltre, l'art. 6, comma 4 prevede che qualora vi sia motivo di dubitare dell'identità personale dello straniero, questi sia sottoposto a rilievi fotodattiloscopici e segnaletici.

possa essere condizionata dalla struttura dell'archivio di riferimento. Se determinate categorie di soggetti sono presenti nella banca dati in misura significativamente maggiore rispetto ad altre, anche un sistema formalmente neutro può produrre effetti indirettamente diseguali. Il rischio di essere sottoposti a identificazione biometrica, di comparire tra i possibili candidati restituiti dal sistema o di subire le conseguenze di un falso positivo non risulta, infatti, distribuito in modo uniforme. In questa prospettiva, la discriminazione algoritmica non dipende soltanto dal funzionamento interno del software, ma anche dal contesto normativo e amministrativo che alimenta i dati sui quali esso opera¹⁵³.

SARI Real Time, invece, è progettato per consentire l'identificazione biometrica in tempo reale delle persone riprese da sistemi di videosorveglianza, mediante il confronto immediato con banche dati di immagini segnaletiche. In tale ipotesi, il sistema analizza in modo continuativo i flussi video provenienti da telecamere installate in luoghi pubblici o aperti al pubblico e genera segnalazioni automatiche nel caso in cui individui una possibile corrispondenza con uno dei soggetti presenti negli archivi di riferimento¹⁵⁴. Rispetto a SARI Enterprise, dunque, il livello di invasività risulta più elevato, poiché il trattamento biometrico non interviene solo su una immagine già acquisita in sede investigativa, ma si inserisce nel controllo immediato e potenzialmente generalizzato dello spazio pubblico.

Proprio in relazione al SARI Real Time, il Garante per la protezione dei dati personali, con parere del 25 marzo 2021¹⁵⁵ ha espresso significative riserve circa la compatibilità del sistema con il quadro normativo vigente in materia di protezione dei dati personali.

L'Autorità ha anzitutto qualificato il trattamento come trattamento di dati biometrici finalizzato all'identificazione univoca della persona e, dunque, rientrante tra le categorie particolari di dati personali. In ragione della particolare sensibilità di tali dati, il Garante ha ritenuto necessaria una base normativa chiara, specifica e proporzionata,

¹⁵³ Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, 2021 pag. 219 ss.; cfr. FRA Focus, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019, pag. 27 s.

¹⁵⁴ V. Garante per la protezione dei dati personali, parere 25 marzo 2021, n. 127, *Sistema SARI Real Time*, doc. web n. 9575877.

¹⁵⁵ V. Garante privacy, provv. 25 marzo 2021, n. 127, *Parere sul sistema SARI Real Time*, doc. web n. 9575877; Cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 158, 240 ss.

idonea a disciplinare puntualmente finalità, presupposti, modalità e limiti di utilizzo della tecnologia. In assenza di una disciplina espressa sull'identificazione biometrica in tempo reale negli spazi pubblici, l'impiego di SARI Real Time avrebbe attribuito all'autorità un margine di discrezionalità eccessivamente ampio, incompatibile con i principi di legalità, necessità e proporzionalità.

Secondo il Garante, la base normativa risultava insufficiente o comunque non sufficientemente determinata in quanto l'ordinamento italiano non prevedeva una disciplina espressa in grado di regolamentare l'utilizzo di sistemi di riconoscimento facciale in tempo reale negli spazi pubblici e per finalità di pubblica sicurezza¹⁵⁶. Mancando tale disciplina, l'impiego di tecnologie di identificazione biometrica diffusa rischierebbe di incidere significativamente sui diritti e le libertà fondamentali degli individui.

Il ragionamento del Garante si fonda su alcuni principi cardine di diritto europeo sulla protezione dei dati personali:

- 1) Principio di necessità, per cui il trattamento deve risultare come strettamente indispensabile alle finalità perseguite.
- 2) Principio di proporzionalità, che impone di valutare se i benefici derivanti dall'utilizzo della tecnologia siano tali da giustificare l'incidenza sui diritti fondamentali degli interessati.
- 3) Principio di minimizzazione dei dati, che richiede di limitare il trattamento ai soli dati strettamente necessari rispetto alle finalità perseguite¹⁵⁷.

Alla luce di questi principi, l'Autorità ha osservato come l'identificazione biometrica in tempo reale negli spazi pubblici possa tradursi in una forma di sorveglianza

¹⁵⁶ V. Garante privacy, parere 25 marzo 2021, doc. web n. 9575877; Cfr. G. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *La Legislazione Penale* (www.lalegislationepenale.eu), dicembre 2021, pag. 6 ss.

¹⁵⁷ V. Garante privacy, doc. web n. 9575877; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 172, 245

generalizzata della popolazione¹⁵⁸, suscettibile di incidere non solo sul diritto alla protezione dei dati personali, ma anche su altre libertà fondamentali.

Le criticità evidenziate dal Garante hanno trovato riscontro anche nell'intervento del legislatore italiano¹⁵⁹, che con il decreto-legge n. 139 del 2021, convertito nella legge n. 205 del 2021, ha introdotto una moratoria sull'utilizzo dei sistemi di riconoscimento facciale negli spazi pubblici fino all'adozione di una disciplina normativa specifica e comunque fino alla definizione del quadro normativo europeo in materia di intelligenza artificiale. Tale intervento conferma come, nel contesto italiano, l'impiego di sistemi di identificazione biometrica in tempo reale continui a sollevare rilevanti questioni di compatibilità con il sistema di tutela dei diritti fondamentali.

Il caso SARI, dunque, mette in luce una duplice criticità. Da un lato, SARI Real Time evidenzia il problema del fondamento normativo dell'identificazione biometrica in tempo reale nello spazio pubblico e il rischio di trasformare la sorveglianza in una pratica generalizzata. Dall'altro lato, SARI Enterprise mostra che anche l'uso differito del riconoscimento facciale può sollevare questioni rilevanti, quando il confronto biometrico avviene rispetto a banche dati non neutrali e caratterizzate da una composizione disomogenea¹⁶⁰.

L'introduzione dei sistemi di identificazione automatizzata pone interrogativi rilevanti sotto il profilo della tutela dei diritti fondamentali in quanto tali tecnologie sono potenzialmente in grado di modificare significativamente i rapporti tra potere pubblico, tecnologia e libertà individuali¹⁶¹. In tale prospettiva, l'evoluzione

¹⁵⁸ V. Garante privacy, comunicato stampa 16 aprile 2021, *Riconoscimento facciale: Sari Real Time non è conforme alla normativa sulla privacy* in cui si afferma che il sistema, per come progettato, realizzerebbe una forma di sorveglianza indiscriminata.

¹⁵⁹ V. art. 9, d.l. 8 ottobre 2021, n. 139, conv. con modifica dalla l. 3 dicembre 2021, n. 205, *recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali*; cfr. Garante privacy, *Relazione annuale 2020* nella parte in cui l'Autorità già segnalava le criticità dell'impiego degli strumenti biometrici e di riconoscimento facciale, prefigurando l'esigenza di un più chiaro presidio normativo.

¹⁶⁰ V. Garante privacy, parere 25 marzo 2021, doc. web n. 9575877; cfr. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, adottato il 26 aprile 2023 pag. 5 s, 14 ss.; Cfr. V. PAGNANELLI, *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, in Osservatorio sulle fonti (www.osservatoriosullefonti.it), n. 2/2021, pag. 788 s., 800 ss.

¹⁶¹ Cfr. A. MANTELERO, *Artificial Intelligence, dati e diritti: spunti di riflessione per i regolatori*, in P. Bertoli, F. Ferrari, G. Ripamonti, G. Tiberi (a cura di), *Data protection tra Unione europea, Italia e Svizzera*, Giappichelli editore, 2019, pag. 24 s.

successiva del caso SARI appare particolarmente significativa perché consente di verificare se le criticità evidenziate dal Garante nel 2021 abbiano trovato un successivo superamento sul piano sia normativo che applicativo, oppure se, al contrario, esse continuino a segnare il quadro giuridico italiano in materia di riconoscimento facciale. Gli sviluppi successivi sembrano confermare la perdurante attualità delle riserve che erano già state formulate dall'Autorità: dopo il parere sfavorevole del marzo 2021, infatti, non risulta l'introduzione di una disciplina legislativa sufficientemente specifica e dettagliata che sia idonea a legittimare l'identificazione biometrica in tempo reale nei luoghi pubblici o aperti al pubblico. Al contrario, il legislatore ha mantenuto un approccio prudentiale, prorogando la sospensione dell'installazione e dell'utilizzo di impianti di videosorveglianza con sistemi di riconoscimento facciale fino a dicembre 2027¹⁶². La scelta normativa in questione sembra confermare, quindi, che allo stato degli atti le condizioni di legalità richieste per un impiego di simili sistemi in ambito pubblico non possano ancora dirsi compiutamente realizzate.

Ciò non significa, tuttavia, che il caso SARI sia da considerarsi definitivamente esaurito. Se SARI Real Time continua a rappresentare il punto più evidente di frizione con i principi di legalità, necessità e proporzionalità, il dibattito si è esteso anche a SARI Enterprise: le informazioni emerse successivamente tramite iniziative di accesso civico e ricostruzioni giornalistiche hanno evidenziato un ricorso quantitativamente significativo a tale applicativo¹⁶³, inoltre, i dati più recenti sulla composizione della banca dati A.F.I.S. mostrano che la questione non si esaurisce nel divieto di identificazione in tempo reale ma investe la trasparenza amministrativa, la verificabilità dell'efficacia del sistema, la misurazione dei falsi positivi e la

¹⁶² V. Garante privacy, provv. n. 127/2021 doc. web n. 9575877; v. art. 9, co. 9, del d.l. 8 ottobre 2021, n. 139, conv. con modifica dalla l. 3 dicembre 2021, n. 205, come modificato dall'art. 12, co. 6-quater, della l. 27 febbraio 2026, n. 26; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 243 s.

¹⁶³ Cfr. StraLi (www.strali.org), *Il caso trasparenza*, ove si riferisce che, a seguito della richiesta di riesame proposta nei confronti del diniego opposto all'accesso civico generalizzato, la Direzione competente del Ministero dell'Interno ha comunicato, per la prima volta, il numero di ricerche effettuate nel Sistema SARI negli anni 2022 e 2023, rispettivamente pari a 79.362 e 131.023; cfr R. COLUCCINI, A. GIANNINI, L. SOTTILE, *Il Viminale ci tiene all'oscuro su come e quanto usa il sistema di riconoscimento facciale*, in IrpiMedia (www.irpimedia.irpi.eu), luglio 2024

predisposizione di adeguate garanzie rispetto all'uso investigativo delle tecnologie biometriche¹⁶⁴.

4.1.1 *I più recenti sviluppi dell'attuazione nazionale dell'AI Act in materia di identificazione biometrica*

Successivamente alla redazione del presente capitolo, il quadro normativo nazionale relativo all'impiego dell'intelligenza artificiale nelle attività di polizia è stato interessato da un significativo sviluppo. In attuazione della delega contenuta nell'articolo 24 della legge n. 132/2025, il Governo ha infatti predisposto lo schema di decreto legislativo recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2024/1689, con particolare riferimento all'utilizzo dei sistemi di intelligenza artificiale nell'attività di polizia e alla responsabilità civile e penale. Lo schema, presentato alle Camere come Atto di Governo n. 418, è stato esaminato dalle competenti Commissioni parlamentari e ha ricevuto in data 30 luglio 2026 un parere favorevole con osservazioni dalle Commissioni riunite 1^a (Affari costituzionali) e 2^a (Giustizia) del Senato¹⁶⁵.

Il Governo ha successivamente comunicato, in data 4 agosto 2026, l'approvazione definitiva del relativo decreto legislativo, precisando che il testo era stato modificato alla luce dei pareri espressi dalle Commissioni parlamentari, dalla Conferenza unificata e dal Garante per la protezione dei dati personali¹⁶⁶. Il decreto legislativo 9 settembre 2026, n. 160, pubblicato nella Gazzetta Ufficiale del 15 settembre 2026, entrerà in vigore il 30 settembre 2026.

La disciplina assume particolare rilievo con riferimento all'identificazione biometrica remota in tempo reale, che costituisce uno degli ambiti di maggiore incidenza sui diritti fondamentali tra quelli interessati dall'intervento nazionale. L'articolo 8 del decreto disciplina, infatti, le condizioni per l'utilizzo, da parte delle Forze di polizia, di sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale in

¹⁶⁴ Cfr. Memoria del Presidente del Garante privacy, prof. P. Stanzione, *Indagine conoscitiva sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano*, Camera dei deputati, X Commissione, 7 febbraio 2024, doc. web n. 9982816

¹⁶⁵ V. Senato della Repubblica, Resoconto sommario n. 93, 30 luglio 2026

¹⁶⁶ Cfr. Presidenza del Consiglio dei Ministri, Comunicato stampa del Consiglio dei Ministri n. 185, voce "intelligenza artificiale"

luoghi pubblici o aperti al pubblico. L'impiego è circoscritto a specifiche finalità di prevenzione e ricerca, individuate:

- a) Nella prevenzione di determinate minacce
- b) Nella ricerca di persone scomparse o vittime di specifici reati¹⁶⁷

La disposizione stabilisce, inoltre, che l'identificazione possa essere utilizzata esclusivamente per la conferma dell'identità delle persone interessate ovvero per la ricerca mirata di persone specificamente individuate o individuabili in relazione alla minaccia da prevenire o alla ricerca da effettuare. Ne deriva l'esclusione di forme generalizzate e indiscriminate di identificazione biometrica, coerentemente con il perimetro delineato dall'articolo 5, paragrafo 1, lettera h) del Regolamento (UE) 2024/1689¹⁶⁸.

Particolare rilievo assume, inoltre, la disciplina della banca dati di riferimento: il confronto biometrico deve essere effettuato mediante una banca dati adeguata alla specifica finalità perseguita, mentre è espressamente escluso l'utilizzo di banche dati biometriche alimentate mediante tecniche di scraping non mirato, ovvero costituite in violazione della normativa in materia di protezione dei dati personali¹⁶⁹. Tale previsione assume una rilevanza ulteriore alla luce delle osservazioni formulate dalla prima e seconda Commissione del Senato riunite, le quali hanno richiesto di precisare la natura della banca dati di riferimento e di definirne i requisiti minimi in termini di accuratezza, affidabilità, sicurezza, tempi di cancellazione e garanzie di non incrementabilità del set di confronto per ciascun utilizzo autorizzato¹⁷⁰.

¹⁶⁷ V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 8

¹⁶⁸ V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 8; v. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*, art. 5, par. 1, lett. h)

¹⁶⁹ V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 8

¹⁷⁰ V. Senato della Repubblica, Resoconto sommario n. 93, 30 luglio 2026

La disciplina prevede altresì specifiche garanzie procedurali. L'utilizzo dei sistemi – limitatamente alle finalità appena descritte – è subordinato a una richiesta al Procuratore della Repubblica presso il tribunale del capoluogo del distretto, contenente l'indicazione della finalità perseguita, della durata prevista, dell'area territoriale interessata, delle persone interessate o ricercate, delle banche dati di riferimento e dei sistemi e delle tecnologie impiegati, nonché alla relativa autorizzazione. Sono poi individuate specifiche condizioni per l'attivazione in situazioni di emergenza, mentre l'inosservanza dei presupposti e dei termini stabiliti comporta la cessazione dell'utilizzo del sistema, la cancellazione dei dati, dei risultati e degli output acquisiti e l'inutilizzabilità dei risultati ottenuti¹⁷¹.

A tali garanzie si aggiungono quelle previste dall'articolo 9 del decreto legislativo n. 160/2026, che introduce una serie di obblighi di carattere procedurale e tecnico tra cui la valutazione di impatto sui diritti fondamentali e la valutazione di impatto sulla protezione dei dati personali, la registrazione delle operazioni mediante appositi file di log non modificabili e la conservazione degli stessi per cinque anni, nonché la notifica al Garante per la protezione dei dati personali dell'avvenuto impiego dei sistemi¹⁷². Il Garante, nel proprio parere del 14 luglio 2026, ha sottolineato la necessità di assicurare un adeguato livello di garanzie rispetto al trattamento dei dati personali connesso all'impiego dell'intelligenza artificiale nelle attività di polizia, richiamando altresì il ruolo della sorveglianza umana e il necessario coordinamento con il Regolamento (UE) 2024/1689 e con il decreto legislativo 51/2018¹⁷³.

Accanto alla disciplina dell'identificazione biometrica remota in tempo reale, l'intervento normativo distingue espressamente l'ipotesi di riconoscimento facciale a posteriori. L'articolo 10 del decreto disciplina, infatti, l'integrazione di componenti di intelligenza artificiale nei sistemi di videosorveglianza già legittimamente installati,

¹⁷¹ V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 8, comma 4

¹⁷² V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 9, comma 1

¹⁷³ Cfr. Garante privacy, provvedimento n. 531 del 14 luglio 2026, doc. web 10275606

allo scopo di consentire l'attivazione successiva della tecnologia di riconoscimento facciale. Si tratta, pertanto, di un utilizzo strutturalmente diverso dall'identificazione biometrica remota in tempo reale in quanto l'elaborazione biometrica viene effettuata successivamente rispetto all'acquisizione delle immagini¹⁷⁴.

L'utilizzo a posteriori è a sua volta circoscritto alle ipotesi successive alla commissione di un reato. Quando il riconoscimento facciale è impiegato per la ricerca mirata di una persona indiziata della commissione di un reato, il Pubblico Ministero richiede al giudice per le indagini preliminari l'autorizzazione all'utilizzo del sistema. È, invece, esclusa la necessità di tale autorizzazione quando la tecnologia è impiegata esclusivamente per l'identificazione iniziale di una persona potenzialmente indiziata della commissione del reato, sulla base di elementi oggettivi e verificabili direttamente connessi al fatto. La disposizione esclude inoltre l'utilizzo dei sistemi per decisioni produttive di effetti giuridici negativi fondate unicamente sui risultati del riconoscimento facciale, nonché per forme di identificazione biometrica generalizzata, non mirata e priva di collegamento con un reato o con un procedimento penale¹⁷⁵.

Un'ulteriore distinzione, particolarmente rilevante sul piano processuale, è contenuta nell'articolo 13 del decreto 160/2026 che introduce nel Codice di procedura penale il nuovo articolo 359-ter. La disposizione non configura una diversa tecnologia di identificazione biometrica, ma disciplina uno specifico contesto processuale di impiego della medesima tecnologia, qualificandola come mezzo di ricerca della prova nell'ambito delle indagini preliminari¹⁷⁶. In questo caso, quindi, l'identificazione biometrica remota in tempo reale non è impiegata come strumento generale di prevenzione, ma nell'ambito di un procedimento penale già instaurato e per specifiche

¹⁷⁴ V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 10

¹⁷⁵ V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 10, commi 2 e 3; cfr. Garante privacy, provvedimento n. 531 del 14 luglio 2026, doc. web 10275606

¹⁷⁶ V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 13

finalità investigative come la conferma dell'identificazione o la ricerca mirata di un indiziato, anche mediante localizzazione, ovvero la ricerca di un latitante destinatario di una misura cautelare o di un ordine di esecuzione¹⁷⁷.

Proprio tale distinzione consente di comprendere come la locuzione “identificazione biometrica in tempo reale” individui una modalità tecnologica di trattamento e non una specifica finalità giuridica. Tale tecnologia può infatti essere impiegata, entro i limiti stabiliti dall'ordinamento, per finalità preventive e di ricerca ai sensi dell'articolo 8, ovvero per finalità investigative nell'ambito delle indagini preliminari secondo la disciplina processuale introdotta dall'articolo 13. Nel secondo caso, la particolare incidenza del trattamento sui diritti fondamentali giustifica l'introduzione di una specifica disciplina processuale e della necessità di autorizzazione del giudice per le indagini preliminari.

Nel complesso l'intervento normativo segna il passaggio da una disciplina fondata sui principi generali della protezione dei dati personali e sulla normativa di settore, a una regolamentazione maggiormente specifica dell'impiego dei sistemi di identificazione biometrica nelle attività di Polizia.

Tale normativa assume particolare rilievo proprio in relazione a SARI Real Time, le cui caratteristiche funzionali risultano riconducibili alla nozione di identificazione biometrica remota in tempo reale disciplinata dall'articolo 8 del decreto legislativo 160/2026¹⁷⁸. La riconducibilità del sistema a tale categoria tecnologica, tuttavia, non consente di ritenere automaticamente lecito il suo impiego in quanto occorre verificare in concreto la specifica finalità perseguita, la sussistenza dei presupposti normativi e il rispetto delle garanzie previste dalla disciplina europea e nazionale.

¹⁷⁷ V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 13; cfr. Garante privacy, provvedimento n. 531 del 14 luglio 2026, doc. web 10275606

¹⁷⁸ V. d.lgs. 9 settembre 2026, n. 160 (Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale), art. 8

4.2 Il caso Clearview AI

Ulteriore passaggio nell'elaborazione della posizione del Garante è il provvedimento adottato nei confronti della società americana Clearview AI¹⁷⁹. Tale società ha sviluppato un sistema di riconoscimento facciale basato sulla creazione di un vasto database biometrico ottenuto tramite la raccolta automatizzata di immagini presenti sui social network e internet: tramite tecniche di scraping¹⁸⁰ Clearview ha raccolto miliardi di fotografie online e le ha trasformate in template biometrici utilizzati, in seguito, per identificare le persone ritrattevi.

Con un provvedimento del 10 febbraio 2022¹⁸¹ il Garante ha accertato che l'attività della società in questione comportava un trattamento illecito di dati personali anche di cittadini italiani. L'Autorità, di conseguenza ha disposto il divieto di ulteriore trattamento di dati relativi agli italiani, la cancellazione dei dati già raccolti e l'irrogazione di una sanzione amministrativa cospicua.

Nella motivazione del provvedimento, il Garante ha evidenziato delle violazioni del GDPR, tra cui l'assenza di una base giuridica idonea per il trattamento, la violazione dei diritti di trasparenza e informazione degli interessati, il trattamento illecito di dati biometrici e la mancata designazione di un rappresentante nell'Unione europea¹⁸². Particolarmente significativo risulta il passaggio del provvedimento ove si afferma che la mera pubblicazione di immagini su internet non implica la legittimazione del loro utilizzo per finalità di identificazione biometrica¹⁸³: la disponibilità pubblica di un dato non equivale alla sua riutilizzabilità per qualunque scopo. Il principio si inserisce nel

¹⁷⁹ V. Garante privacy, ord. ingiunzione n. 50 del 10 febbraio 2022, doc. web 9751362

¹⁸⁰ Con scraping, in genere, si intende quell'attività automatizzata di estrazione e raccolta di dati da siti web, piattaforme online o contenuti disponibili in rete, che viene fatta tramite software o script in grado di acquisire in modo massivo informazioni. Nel contesto del riconoscimento facciale questa tecnica è stata usata per reperire immagini pubblicate online e trasformarle in dati biometrici mediante successiva elaborazione algoritmica.

Cfr. I.N. REZENDE, *Facial recognition in police hands: Assessing the "Clearview case" from a European perspective*, New Journal of European Criminal Law, vol. 11 n. 3, 2020, pag. 376 s.

¹⁸¹ V. Garante privacy, ord. ingiunzione n. 50/2022, doc. web 9751362, nonché comunicato stampa del Garante privacy del 9 marzo 2022, *riconoscimento facciale: il Garante privacy sanziona Clearview per 20 milioni di euro. Vietato l'uso dei dati biometrici e il monitoraggio degli italiani*

¹⁸² V. Garante privacy, ord. ingiunzione n. 50/2022, doc. web 9751362

¹⁸³ V. Garante privacy, ord. ingiunzione n. 50/2022, doc. web 9751362; cfr. N. REZENDE, *Facial recognition in police hands: Assessing the "Clearview case" from a European perspective* New Journal of European Criminal Law vol. 11 n. 3, 2020, pag. 379 s.

solco della teoria dell'autodeterminazione informativa per cui l'interessato deve mantenere un controllo sostanziale sulle modalità di utilizzo dei suoi dati personali¹⁸⁴.

Il significato del provvedimento adottato dal Garante italiano risulta, peraltro, più evidente se collocato nel contesto europeo: la decisione del febbraio 2022 ha infatti segnato, nel nostro ordinamento, una presa di posizione molto netta nei confronti del modello operativo di Clearview AI fondato sulla raccolta massiva di immagini reperite online e sul loro successivo trattamento a fini di identificazione biometrica¹⁸⁵. Nondimeno, nelle successive fonti istituzionali non emergono elementi tali da consentire di ritenere integralmente definita la vicenda sotto il profilo dell'effettività concreta delle misure impartite nei confronti della società. Tale dato però non pregiudica o ridimensiona la portata del provvedimento, ma ne conferma il rilievo sistemico in quanto evidenzia le difficoltà che l'applicazione territoriale del GDPR incontra nei confronti di quegli operatori che sono stabiliti al di fuori dell'Unione europea.

Nonostante ciò, la posizione del Garante italiano non è rimasta isolata, ma si è inserita in un orientamento europeo convergente in cui anche altre Autorità nazionali di protezione dei dati personali hanno contestato a Clearview AI l'illiceità del trattamento di dati biometrici ricavati tramite scraping di immagini online e hanno adottato nei suoi confronti misure sanzionatorie e correttive di particolare severità¹⁸⁶. Il caso in esame, quindi, assume un rilievo che trascende la singola iniziativa nazionale e rappresenta uno dei più significativi banchi di prova della capacità delle Autorità europee di reagire ai modelli di riconoscimento facciale che si basano sulla raccolta indiscriminata di dati personali reperiti sul web.

¹⁸⁴ Cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, 2021, pag. 78 ss.; e in prospettiva europea, EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, adottato il 26 aprile 2023 pag. 10, 22 ss.

¹⁸⁵ V. Garante privacy, ord. ingiunzione n. 50/2022, doc. web 9751362; v. EDPB, *Facial recognition: Italian SA fines Clearview AI EUR 20 milion*, 10 marzo 2022

¹⁸⁶ Cfr. EDPB, *Hellenic DPA fines Clearview AI 20 milion euros*, 20 luglio 2022; cfr. EDPB, *The french SA fines Clearview AI EUR 20 milion*, 20 ottobre 2022; cfr. EDPB, *Decision by the Austrian SA against Clearview AI. Infringements of Articles 5, 6, 9, 27 GDPR*, 12 maggio 2023; I.N. REZENDE, *Facial recognition in police hands: Assessing the "Clearview case" from a European perspective*, New Journal of European Criminal Law vol. 11 n. 3, 2020, pag. 381 s., 387 ss.

4.3 Le sperimentazioni del riconoscimento facciale negli aeroporti – faceboarding

In questo caso, diversamente dai precedenti, il Garante ha mostrato un atteggiamento più aperto rispetto ad alcune sperimentazioni che utilizzano il riconoscimento facciale¹⁸⁷: si tratta di contesti specifici e circoscritti in cui sono stati usati dei sistemi di faceboarding presso gli aeroporti di Roma Fiumicino e Milano Linate.

I sistemi di faceboarding consentono ai passeggeri di utilizzare il proprio volto come credenziale di identificazione per accedere ai controlli di sicurezza e imbarco, in sostituzione parziale dell'esame dei tradizionali documenti di viaggio¹⁸⁸. Il suo funzionamento prevede la registrazione volontaria del volto da parte del passeggero che, in seguito, viene confrontato con le immagini acquisite durante le varie fasi del percorso aeroportuale.

Nella valutazione di legittimità di queste sperimentazioni il Garante ha optato per un approccio basato sul principio di proporzionalità contestuale e ha individuato una serie di condizioni necessarie per garantire la conformità al GDPR¹⁸⁹. Tra queste condizioni troviamo la volontarietà dell'adesione a tale sistema, la possibilità di usare procedure alternative non biometriche, la limitazione temporale della conservazione dei dati biometrici, l'effettuazione di una valutazione di impatto sulla protezione dei dati e l'adozione di adeguate misure di sicurezza tecniche e organizzative.

L'Autorità, inoltre, ha ritenuto che il sistema non determinasse una forma di sorveglianza di massa perché il relativo trattamento avveniva in un contesto delimitato, per finalità specifiche e con il consenso degli interessati. Ciò dimostra che l'Autorità italiana non ha un pregiudizio generalizzato nei confronti delle tecnologie biometriche,

¹⁸⁷ Cfr. Garante privacy, provvedimento n. 513, 12 novembre 2014, come rettificato dal provvedimento n. 16, 15 gennaio 2015, *Provvedimento generale prescrittivo in tema di biometria*, pag. 3.

¹⁸⁸ V. Aeroporto di Milano Linate, *FaceBoarding* (www.milanolinate-airport.com), ove si afferma che il servizio consente ai passeggeri di accedere ai controlli di sicurezza e di effettuare procedure di imbarco mediante riconoscimento facciale, senza necessità di esibire al checkpoint il passaporto o la carte d'identità elettronica e la carta d'imbarco.

¹⁸⁹ Cfr. Garante privacy, provvedimento n. 513, 12 novembre 2014, come rettificato dal provvedimento n. 16, 15 gennaio 2015, *Provvedimento generale prescrittivo in tema di biometria*, pag. 3 s.; cfr. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, adottato il 26 aprile 2023 pag. 10, 25 ss.

ma ne valuta l'ammissibilità in seguito a una verifica concreta dei rischi per i diritti fondamentali¹⁹⁰.

Il rilievo del caso, tuttavia, non si esaurisce in questa prima fase di apertura condizionata. La vicenda del faceboarding, infatti, ha conosciuto un'evoluzione successiva che ha contribuito a precisare su scala europea e nazionale le condizioni di liceità del ricorso al riconoscimento facciale per finalità di agevolazione dei flussi di transito dei passeggeri¹⁹¹. In particolare, il Comitato europeo per la protezione dei dati personali, con il parere n. 11/2024 ha chiarito che simili sistemi possono ritenersi compatibili con il GDPR solo in presenza di specifiche architetture tecniche idonee ad assicurare all'interessato un controllo effettivo sul template biometrico, mentre risultano incompatibili con la disciplina europea le soluzioni basate su forme di conservazione centralizzata dei dati biometrici sotto il controllo del gestore aeroportuale o della compagnia aerea. In linea con questa impostazione, il Garante italiano, con provvedimento dell'11 settembre 2025, ha disposto la sospensione della soluzione adottata presso l'aeroporto di Milano-Linate, ritenendola non conforme al Regolamento europeo¹⁹².

Ne deriva che il seguito della vicenda non ha condotto né a una generale legittimazione del riconoscimento facciale in ambito aeroportuale, né a una sua assoluta preclusione. Piuttosto, esso ha reso più netti i confini entro cui tali sistemi possono aspirare a un impiego lecito, confermando come il nodo decisivo non risieda nell'astratta finalità di semplificazione del servizio, bensì nelle concrete modalità tecniche e organizzative del trattamento dei dati biometrici¹⁹³. Proprio questo approdo rende il caso particolarmente significativo: il riconoscimento facciale, anche quando si presenta sotto la veste

¹⁹⁰ Cfr. Garante privacy, provvedimento n. 513, 12 novembre 2014, come rettificato dal provvedimento n. 16, 15 gennaio 2015, *Provvedimento generale prescrittivo in tema di biometria*, pag. 3 s.; cfr. EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, version 2.0, adottato il 26 aprile 2023 pag. 10, 25 ss.; cfr. Garante privacy, provvedimento, 11 settembre 2025, doc. web n. 10167745

¹⁹¹ V. EDPB, *Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow*, 23 maggio 2024, pag. 3 ss., 28 ss.

¹⁹² V. Garante privacy, provv. 11 settembre 2025, n. 489, doc. web n. 10167745 in cui il sistema faceboarding viene ricondotto allo scenario 3 dell'Opinion EDPB 11/2024 ed è disposta, con effetto immediato, la limitazione provvisoria del trattamento dei dati biometrici dei passeggeri presso l'aeroporto di Milano-Linate; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 158 s., 172 ss.

¹⁹³ V. Garante privacy, comunicato stampa 18 settembre 2025, doc. web n. 10167973, *Nessun divieto generale all'utilizzo del riconoscimento facciale in aeroporto*

dell'agevolazione dei servizi e dell'efficienza organizzativa, continua a porre questioni centrali di controllo sull'identità personale e di tutela dei diritti fondamentali.

4.4 Il riconoscimento facciale e i rapporti tra privati

Il tema del riconoscimento facciale non rileva solo nei rapporti tra individuo e autorità pubblica, ma si manifesta con particolare intensità anche nei rapporti tra privati e, anche in questo caso, l'identificazione biometrica del volto è suscettibile di incidere su una pluralità di diritti fondamentali. Il trattamento dei dati biometrici in questo ambito, infatti, coinvolge anzitutto la riservatezza e la vita privata in quanto rende la persona identificabile in modo stabile anche in spazi e relazioni della sua quotidianità. Il riconoscimento facciale, inoltre, incide sull'autodeterminazione informativa nella misura in cui sottrae all'interessato il controllo su un dato identitario particolarmente delicato, ma anche sulla dignità della persona in quanto il volto tende a trasformarsi in una credenziale di accesso, verifica o selezione. A ciò si aggiunge il profilo dell'eguaglianza e della non discriminazione dal momento che l'impiego dei sistemi biometrici può produrre esclusioni, trattamenti differenziati o errori che incidono sulla posizione giuridica dell'interessato.

Le linee guida 03/2019 dell'EDPB mostrano bene tali problematiche e sottolineano che l'uso intensivo di dispositivi video muniti di funzionalità biometriche da parte di privati rende più difficile rimanere anonimi e può favorire usi secondari o impropri dei dati, quindi, comporta rischi elevati per i diritti e le libertà degli interessati¹⁹⁴.

Nel quadro giuridico italiano questi rischi sono affrontati muovendo dalla particolare delicatezza del dato biometrico, quindi, dalla necessità che il suo trattamento sia sorretto da un'adequata base giuridica e che sia comunque conforme ai principi di liceità, necessità, proporzionalità e minimizzazione. Per questa ragione, il ricorso a tecnologie biometriche non può essere considerato una modalità ordinaria di organizzazione dei rapporti tra privati, ma richiede una giustificazione rafforzata, soprattutto quando la stessa finalità può essere perseguita con strumenti meno invasivi. Inoltre, assume rilievo anche la questione della modalità di conservazione del dato

¹⁹⁴ Cfr. M. QUARANTA, *I sistemi di rilevazione di accessi e presenze con l'uso di dati biometrici sul posto di lavoro*, in *Diritto, Economia e Tecnologie della Privacy*, anno VI, n. 3, 2015, pag. 331 s.; cfr. EDPB, *Guidelines 03/2019 on processing of personal data through video devices*, version 2.0, pag. 5 s., 17 ss.

biometrico in quanto la creazione di archivi centralizzati accresce i rischi legati al riutilizzo dei dati, ai collegamenti con ulteriori banche dati e, più in generale, alla perdita di controllo dell'interessato sul proprio dato identitario¹⁹⁵.

Una conferma particolarmente significativa di questa impostazione si rinviene anche nella più recente prassi del Garante privacy in materia di utilizzo del riconoscimento facciale sul luogo di lavoro. L'Autorità, infatti, ha chiarito che l'impiego del volto dei dipendenti per la rilevazione delle presenze comporta un trattamento di dati biometrici sia nella fase di registrazione iniziale del lavoratore, sia in quella successiva di riconoscimento in sede di timbratura. Proprio per questo, un simile trattamento non si può ritenere automaticamente lecito, ma richiede la ricorrenza delle condizioni di cui all'articolo 9 del GDPR, oltre al rispetto dei principi di proporzionalità e necessità. Nella stessa prospettiva, il Garante, ha valorizzato il fatto che la finalità di verifica della presenza, di regola, può essere perseguita tramite strumenti meno invasivi, quindi il ricorso al riconoscimento facciale finisce per eccedere lo scopo perseguito¹⁹⁶.

Del resto, l'approccio restrittivo emerso nella prassi del Garante è in linea con la giurisprudenza della Corte europea dei diritti dell'uomo in materia di monitoraggio del lavoratore in cui si afferma che anche nel rapporto di lavoro tra privati il controllo tecnologico del lavoratore ricade nell'ambito di tutela dell'articolo 8 della CEDU. In *Bărbulescu c. Romania*, la Grande camera ha chiarito che la compatibilità di simili forme di monitoraggio richiede una verifica particolarmente attenta che tenga conto della previa informativa resa al lavoratore, della natura e dell'estensione del controllo, delle ragioni che lo giustificano, della possibilità di ricorrere a misura meno invasive e delle conseguenze prodotte nella sua sfera personale. In *López Ribalda and Others c. Spain*, la stessa Corte ha ribadito che anche la videosorveglianza sul luogo di lavoro deve essere sottoposta a un rigoroso giudizio di proporzionalità. Se ciò vale con riferimento a strumenti di controllo video, tanto più delicato risulta il ricorso al

¹⁹⁵ V. Garante privacy, *Allegato A al provvedimento generale prescrittivo in tema di biometria*, 12 novembre 2014, n. 513; cfr. M. QUARANTA, *I sistemi di rilevazione di accessi e presenze con l'uso di dati biometrici sul posto di lavoro*, in *Diritto, Economia e Tecnologie della Privacy*, anno VI, n. 3, 2015, pag. 333 ss.

¹⁹⁶ V. Garante privacy, provv. n. 105, 106, 107, 108, 109 del 2024; cfr. G.M. MARSICO, *Violazione della normativa in tema di privacy e riservatezza: profili ricostruttivi sul divieto di riconoscimento facciale dei dipendenti ai fini della verifica delle presenze sul posto di lavoro*, in *RivistaLabor* (www.rivistalabor.it), 13 maggio 2024, pag. 1 s., 6 ss.

riconoscimento facciale, in cui il monitoraggio si basa sul trattamento automatizzato di dati biometrici idonei a identificare univocamente la persona¹⁹⁷.

Criticità non minori emergono anche nell'accesso a beni o servizi privati, in particolare in contesti quali strutture ricettive, esercizi commerciali, ambienti ad accesso selettivo o altri spazi in cui il riconoscimento facciale tende a essere presentato come strumento di sicurezza o di semplificazione di un servizio. In queste ipotesi, tuttavia, l'identificazione biometrica non può considerarsi una modalità neutra di organizzazione del rapporto in quanto condiziona l'accesso a spazi e prestazioni tramite il trattamento di un dato che è idoneo a identificare in modo univoco una persona. Vengono pertanto in rilievo la riservatezza e l'autodeterminazione informativa dell'interessato in quanto vede ridursi la possibilità di fruire del servizio se non identificato biometricamente, ma anche l'eguaglianza ove l'impiego dei sistemi di riconoscimento facciale può determinare esclusioni, trattamenti differenziati o svantaggi derivanti da errori, bias o malfunzionamenti algoritmici¹⁹⁸.

Le linee guida 03/2019 dell'EDPB si muovono proprio in questa direzione e chiariscono che l'utilizzo di funzionalità biometriche da parte di soggetti privati comporta rischi particolarmente elevati per i diritti e le libertà degli interessati e richiede, perciò, un vaglio rigoroso sotto il profilo della necessità, della proporzionalità e della minimizzazione. Nello specifico, il Comitato ha evidenziato come il trattamento biometrico non possa essere imposto come modalità ordinaria di accesso al servizio quando la medesima finalità possa essere perseguita tramite strumenti alternativi meno invasivi, e sottolinea anche i rischi specifici connessi alla raccolta dei dati biometrici in ambienti che non sono controllati e, per questo possono essere coinvolti anche soggetti che non hanno espresso alcuna volontà di aderire a questa forma di identificazione¹⁹⁹.

¹⁹⁷ V. Corte EDU, Grande Camera, sent. 5 settembre 2017, *Bărbulescu c. Romania*, ric. n. 61496/08, in Hudoc (www.hudoc.echr.coe.int); Corte EDU, Grande Camera, sent. 17 ottobre 2019, *López Ribalda e a. c. Spagna*, ric. nn. 1874/13 e 8567/13, in Hudoc (www.hudoc.echr.coe.int)

¹⁹⁸ V. EDPB, *Guidelines 03/2019 on processing of personal data through video devices*, version 2.0, pag. 17 ss.; cfr. E. A. ROWE, *Regulation facial recognition technology in the private sector*, in *Stanford technology law review*, vol. 24:1, 2020, pag. 24 ss.

¹⁹⁹ V. EDPB, *Guidelines 03/2019 on processing of personal data through video devices*, version 2.0, pag. 18 ss.

In questa prospettiva si può cogliere, in termini generali, il profilo più delicato del riconoscimento facciale nei rapporti tra privati: ove il trattamento biometrico è introdotto come strumento di comodità o di migliore organizzazione del servizio, e non più come misura eccezionale, il rischio non riguarda solo il singolo trattamento che può essere sproporzionato, ma anche la progressiva trasformazione di una tecnica altamente invasiva come prassi ordinaria. In questo modo, la compressione dei diritti fondamentali non si manifesta tramite evidenti coercizioni, ma può realizzarsi in modi più sottili tramite meccanismi che in apparenza sono funzionali ed efficienti e che, proprio per questo, tendono a rendere usuale il ricorso all'identificazione biometrica. Il riconoscimento facciale nei rapporti tra privati, dunque, conferma che la tutela dei diritti fondamentali non può essere letta in termini unicamente pubblicistici in quanto anche le forze economiche e tecnologiche private sono in grado di incidere profondamente sulla sfera personale, restringendo spazi dell'anonimato e ridefinendo i confini della riservatezza, dell'autodeterminazione e della dignità individuale²⁰⁰.

4.5 Tra prudenza e principi, l'approccio del Garante privacy al riconoscimento facciale

L'analisi di questi casi consente di cogliere come l'elaborazione del pensiero del Garante privacy in materia di riconoscimento facciale non si lasci racchiudere in una formula unica o in un atto generale di indirizzo, ma emerga progressivamente tramite pareri, provvedimenti e interventi adottati in contesti differenti. Proprio questa ricostruzione consente di individuare alcune costanti che restituiscono una visione sufficientemente unitaria dell'approccio seguito dall'Autorità²⁰¹.

In primo luogo, il Garante privacy opta per una particolare cautela nei confronti delle tecnologie di identificazione biometrica, soprattutto se collocate in contesti in cui il trattamento rischia di assumere caratteri diffusi, sistematici o difficilmente controllabili. In questi casi, il punto non è solo l'efficienza dello strumento o la sua utilità pratica, ma il fatto che le tecnologie di riconoscimento facciale, trasformando il volto in un dato trattabile e confrontabile automaticamente, espone la persona a una

²⁰⁰ V. EDPB, *Guidelines 03/2019 on processing of personal data through video devices*, version 2.0, pag. 5 s.; cfr. E. A. ROWE, *Regulation facial recognition technology in the private sector*, in *Stanford technology law review*, vol. 24:1, 2020, pag. 24 ss.

²⁰¹ V. Memoria del Presidente del Garante Privacy, *Indagine conoscitiva sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano*, 7 febbraio 2024, doc. web n. 9982816

forma di identificazione penetrante che può incidere significativamente sulla sua sfera giuridica²⁰².

In secondo luogo, emerge che il Garante attribuisce un rilievo decisivo sia alla finalità dichiarata del trattamento sia alle sue concrete modalità di funzionamento. Sotto questo profilo, infatti, si interroga costantemente sulla base giuridica del trattamento, sulla possibilità di ricorrere a strumenti meno invasivi, sulle modalità di conservazione del dato biometrico e sull'effettiva proporzionalità del sistema rispetto allo scopo perseguito. Ne deriva un approccio che non si arresta alla superficie della tecnologia, ma ne verifica la compatibilità sostanziale con la tutela dei diritti e delle libertà fondamentali²⁰³.

Proprio in tale prospettiva hanno acquistato significato anche le differenze tra i casi esaminati. Se, da un lato, il Garante si mostra particolarmente rigoroso nei confronti delle forme di identificazione biometrica in tempo reale o dei modelli basati sulla raccolta massiva e indiscriminata di dati e immagini, dall'altro non esclude a priori ogni possibile impiego di tali sistemi, anzi ne valuta la liceità alla luce delle specifiche condizioni tecniche e organizzative del trattamento. Ciò consente di cogliere un tratto importante del suo orientamento: il problema non è solo se una determinata tecnologia si possa usare, ma come, a quali condizioni e con quali garanzie si possa introdurre in concreto²⁰⁴. Sotto questo punto di vista, l'estensione anche ai rapporti tra privati conferma che la preoccupazione del Garante privacy non si esaurisce dinanzi all'esercizio del potere pubblico. Al contrario, la sua attenzione si rivolge in generale a ogni impiego del riconoscimento facciale in quanto suscettibile di comprimere la riservatezza, l'autodeterminazione e la dignità della persona, anche ove il trattamento

²⁰² V. Garante Privacy, provv. n. 127, 25 marzo 2021, doc. web n. 9575877; v. Garante Privacy, ordinanza-ingiunzione n. 50, 10 febbraio 2022, doc. web n. 9751362; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 25, 57 ss.

²⁰³ V. Garante Privacy, *Provvedimento generale prescrittivo in tema di biometria*, 12 novembre 2014, n. 513, doc. web n. 3556992; cfr. M. QUARANTA, *I sistemi di rilevazione di accessi e presenze con l'uso di dati biometrici sul posto di lavoro*, in *Diritto, Economia e Tecnologie della Privacy*, anno VI, n. 3, 2015, pag. 333 ss.; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 158 s.

²⁰⁴ Cfr. EDPB, *Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow*, 23 maggio 2024; v. Garante Privacy, provv. n. 489, 11 settembre 2025, doc. web n. 10167745; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 243 s.

sia giustificato da esigenze organizzative, di sicurezza o di semplificazione del servizio. Pertanto, emerge una concezione della protezione dei dati personali come presidio trasversale destinato a operare tanto nei confronti dei poteri pubblici, quanto nei confronti delle forze economiche e tecnologiche private²⁰⁵.

Nel complesso, i provvedimenti visti restituiscono l'immagine di un'Autorità che, più che limitarsi a vietare o autorizzare singole applicazioni dei sistemi di riconoscimento facciale, costruisce in via progressiva una linea interpretativa fondata su alcuni principi cardine:

- La natura particolarmente sensibile dei dati biometrici
- La necessità di una base giuridica adeguata
- Il carattere non ordinario del ricorso a tali strumenti
- L'esigenza che ogni forma di impiego del riconoscimento facciale resti sottoposta a un controllo rigoroso di necessità, proporzionalità e compatibilità con i diritti fondamentali²⁰⁶.

²⁰⁵ Cfr. EDPB, *Guidelines 03/2019 on processing of personal data through video devices*, version 2.0, pag. 5 s., 17 ss.; cfr. M. QUARANTA, *I sistemi di rilevazione di accessi e presenze con l'uso di dati biometrici sul posto di lavoro*, in *Diritto, Economia e Tecnologie della Privacy*, anno VI, n. 3, 2015, pag. 331 s.; cfr. G.M. MARSICO, *Violazione della normativa in tema di privacy e riservatezza: profili ricostruttivi sul divieto di riconoscimento facciale dei dipendenti ai fini della verifica delle presenze sul posto di lavoro*, in *RivistaLabor* (www.rivistalabor.it), 13 maggio 2024, pag. 1 s., 8 s.

²⁰⁶ V. Memoria del Presidente del Garante Privacy, *Indagine conoscitiva sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano*, 7 febbraio 2024, doc. web n. 9982816; cfr. G. MOBILIO, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, editoriale scientifica, 2021, pag. 119, 158 s., 287

Capitolo 3

Modelli internazionali di regolazione del riconoscimento facciale

SOMMARIO: 1. Il modello di sorveglianza totale cinese. – 2. Il sistema Aadhaar indiano: identità biometrica e accesso ai servizi. – 3. Giamaica e Kenya: identità digitale nazionale e biometria amministrativa. – 4. Il modello “innovativo” americano. – 5. Il modello russo e il caso Glukhin c. Russia della Corte EDU.

L'analisi condotta ha permesso di ricostruire il quadro normativo europeo e nazionale relativo all'uso dei sistemi di riconoscimento facciale, evidenziando come tali tecnologie incidano profondamente sull'equilibrio tra l'innovazione tecnologica e la tutela dei diritti fondamentali. In particolare, l'esame della disciplina europea e dell'evoluzione dell'ordinamento italiano ha mostrato come il legislatore e le autorità di garanzia tendano ad adottare un approccio cauto volto a subordinare l'utilizzo di strumenti biometrici a rigorosi requisiti di proporzionalità, necessità e tutela dei dati personali²⁰⁷.

Il rapporto tra le tecnologie di identificazione biometrica e i diritti fondamentali non si esaurisce nell'esperienza europea. In molti ordinamenti extraeuropei, infatti, il riconoscimento facciale è stato sviluppato e impiegato secondo logiche normative, politiche e culturali differenti. Per questo motivo, per comprendere in modo più compiuto le potenzialità e i rischi connessi a queste tecnologie, risulta utile dare uno sguardo ad alcune significative esperienze internazionali. L'analisi comparata permette di mettere in evidenza dei modelli di regolazione eterogenei, che spaziano da sistemi di sorveglianza fortemente centralizzati a modelli più frammentati e orientati al mercato.

L'osservazione comparata consente di cogliere con maggiore chiarezza come l'impiego del riconoscimento facciale non dipenda soltanto dalle potenzialità tecniche dello strumento, ma anche dalla forma di Stato, dalla cultura istituzionale e dal modello

²⁰⁷ Cfr. Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, artt. 5, 9 e 35; v. Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, *relativo a regole armonizzate sull'intelligenza artificiale*

di rapporto tra potere pubblico e individuo. Le esperienze straniere prese in esame mostrano infatti soluzioni profondamente diverse: talora orientate alla massimizzazione della sicurezza e del controllo, talaltra caratterizzate da assetti più frammentati o maggiormente sensibili ai limiti posti dalla tutela dei diritti fondamentali. In questa prospettiva, il confronto comparato non serve solo a descrivere modelli differenti, ma anche a mettere meglio a fuoco i tratti e le criticità dell'approccio europeo. Il capitolo prenderà in esame, in particolare, i modelli cinese, indiano, statunitense e russo.

1. *Il modello di sorveglianza totale cinese*

Tra le esperienze internazionali più significative nell'ambito dell'impiego delle tecnologie di riconoscimento facciale, assume rilievo quella della Repubblica Popolare Cinese. In tale contesto, infatti, lo sviluppo e la diffusione dei sistemi di identificazione biometrica si collocano all'interno di un modello di governance tecnologica caratterizzato da una forte integrazione tra politiche di sicurezza pubblica, innovazione digitale e capacità di monitoraggio amministrativo dello Stato²⁰⁸.

Negli ordinamenti europei l'uso delle tecnologie biometriche è generalmente subordinato a criteri rigorosi di necessità, proporzionalità e tutela dei dati personali, mentre nel sistema cinese si caratterizza per un approccio in cui lo sviluppo delle tecnologie digitali viene concepito come parte integrante delle strategie di sicurezza nazionale e di gestione della società²⁰⁹.

Per comprendere la diffusione dei sistemi di riconoscimento facciale nel contesto cinese è necessario innanzitutto considerare la configurazione del sistema costituzionale e la diversa concezione del rapporto tra diritti individuali e potere pubblico²¹⁰.

²⁰⁸ Cfr. K. SHI-KUPFER, M. OHLBERG, *China's digital rise, challenges for Europe*, in Merics papers on China, n. 7, Aprile 2019, pag. 8 ss.; cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in International Journal of Law and Information Technology, vol. 31/2023, pag. 350 s.; cfr. J. A. LEE, P. ZHOU, *FRT regulation in China*, in Cambridge University Press, pag. 242 ss.

²⁰⁹ Cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in International Journal of Law and Information Technology, vol. 31/2023, pag. 359; cfr. K. SHI-KUPFER, M. OHLBERG, *China's digital rise, challenges for Europe*, in Merics papers on China, n. 7, Aprile 2019, pag. 9 s.

²¹⁰ Cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in International Journal of Law and Information Technology, vol. 31/2023, pag. 359; cfr. J. A. LEE, P. ZHOU, *FRT regulation in China*, in Cambridge University Press, pag. 243 s.

Sul piano costituzionale, la Costituzione della Repubblica Popolare Cinese del 1982 riconosce formalmente alcune garanzie che tutelano la persona. In particolare, l'articolo 38 stabilisce che la dignità personale dei cittadini della Repubblica è inviolabile, mentre l'articolo 40 tutela la libertà e la segretezza delle comunicazioni²¹¹. Queste disposizioni, almeno sul piano formale, sembrano riprendere alcuni principi analoghi a quelli presenti negli ordinamenti occidentali, tuttavia, nel sistema costituzionale cinese i diritti individuali non assumono la funzione di limite strutturale all'esercizio del potere pubblico che caratterizza invece i modelli liberaldemocratici. Essi risultano piuttosto inseriti in una cornice istituzionale in cui la tutela dell'ordine sociale, della stabilità politica e dello sviluppo economico rappresenta un obiettivo prioritario dell'azione statale. In altri termini, mentre negli ordinamenti liberaldemocratici i diritti fondamentali operano tradizionalmente come limite all'esercizio del potere pubblico, nel contesto cinese risultano spesso subordinati alle esigenze di ordine pubblico, sicurezza nazionale e sviluppo economico promosse dallo Stato²¹².

Nel contesto cinese, i diritti riconosciuti dalla Costituzione sono generalmente interpretati alla luce del principio della supremazia dell'interesse collettivo, con la conseguenza che le autorità pubbliche dispongono di ampi margini discrezionali nell'adozione di misure finalizzate alla sicurezza e al controllo sociale. In questa prospettiva, il rapporto tra tecnologia e potere pubblico assume caratteristiche profondamente diverse rispetto al contesto europeo: se in Unione europea l'impiego di strumenti di sorveglianza tecnologica è oggetto di un costante bilanciamento con i diritti fondamentali della persona, in Cina le tecnologie digitali sono frequentemente concepite come strumenti funzionali alla realizzazione degli obiettivi di governance statale²¹³.

²¹¹ V. Costituzione della Repubblica Popolare Cinese, artt. 38 e 40.

²¹² Cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 359; cfr. J. A. LEE, P. ZHOU, *FRT regulation in China*, in Cambridge University Press, pag. 242 ss.; cfr. R. CREEMERS, *China's emerging data protection framework*, in *Journal of cybersecurity*, 2022, pag. 1 s.

²¹³ Cfr. J. A. LEE, P. ZHOU, *FRT regulation in China*, in Cambridge University Press, pag. 243; cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 359; cfr. K. SHI-KUPFER, M. OHLBERG, *China's digital rise, challenges for Europe*, in *Merics papers on China*, n. 7, Aprile 2019, pag. 8 ss.

Nonostante sussistano tali differenze strutturali, negli ultimi anni la Cina ha conosciuto un significativo sviluppo della normativa sulla protezione dei dati e della sicurezza delle informazioni, anche in risposta alla crescente digitalizzazione dell'economia e alla diffusione capillare delle tecnologie di raccolta e trattamento dei dati. Un primo intervento organico in tale direzione è la Cybersecurity Law del 2017 che ha introdotto un quadro normativo volto a disciplinare la sicurezza delle reti informatiche e la gestione delle informazioni digitali, imponendo agli operatori di rete specifici obblighi di protezione dei dati e attribuendo alle autorità pubbliche ampi poteri di supervisione sulle infrastrutture informatiche²¹⁴. Successivamente, il legislatore ha adottato ulteriori strumenti normativi per rafforzare la governance dei dati su scala nazionale e tra questi sono particolarmente rilevanti la Data Security Law del 2021, che disciplina il trattamento e la classificazione dei dati secondo criteri legati alla sicurezza nazionale e agli interessi strategici dello Stato, e la Personal Information Protection Law del 2021, che è considerata come il primo testo legislativo cinese dedicato alla tutela delle informazioni personali²¹⁵.

La Personal Information Protection Law introduce una serie di principi che, sotto alcuni profili, presentano analogie con quelli previsti dal regolamento europeo sulla protezione dei dati, tra cui il principio di minimizzazione del trattamento, l'obbligo di informare gli interessati circa le finalità della raccolta dei dati, la necessità di ottenere il consenso per determinate categorie di trattamento e l'obbligo per i titolari del trattamento di adottare adeguate misure di sicurezza²¹⁶. Tuttavia, come evidenziato da vari studiosi, tali meccanismi operano in un quadro normativo nel quale le esigenze di sicurezza pubblica e di interesse statale mantengono una posizione preminente, consentendo alle autorità pubbliche ampi margini di accesso e utilizzo delle informazioni raccolte. In questo senso, la protezione dei dati personali nel sistema cinese non assume la configurazione di un diritto fondamentale pienamente opponibile

²¹⁴ Cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 359 s.; cfr. R. CREEMERS, *China's emerging data protection framework*, in *Journal of cybersecurity*, 2022, pag. 1 s.; v. artt. 41, 42, 44, 76 (5) Cybersecurity Law of the PRC

²¹⁵ Cfr. R. CREEMERS, *China's emerging data protection framework*, in *Journal of cybersecurity*, 2022, pag. 1 s.; cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 359, 363

²¹⁶ Cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 363, 366

allo Stato, ma si inserisce in un quadro di regolazione volto a garantire il controllo e la gestione dei flussi informativi nell'ambito delle politiche di sicurezza e di sviluppo tecnologico del paese²¹⁷.

Accanto a tale contesto normativo istituzionale si è progressivamente sviluppata una vasta infrastruttura di sorveglianza digitale basata sull'impiego diffuso di sistemi di videosorveglianza e di tecnologie di intelligenza artificiale. Negli ultimi due decenni la Repubblica Popolare Cinese ha infatti realizzato una delle più estese reti di monitoraggio elettronico esistenti a livello globale, attraverso progetti nazionali volti all'integrazione tra telecamere di sicurezza, sistemi di analisi automatizzata delle immagini e banche dati biometriche²¹⁸.

Tra le iniziative più rilevanti in questo ambito vi è il cosiddetto "Skynet Project" (Tianwang), un sistema di videosorveglianza su larga scala che consente alle autorità di sicurezza pubblica di monitorare gli spazi urbani attraverso milioni di telecamere connesse a piattaforme di analisi automatizzata delle immagini. A tale progetto si affianca il programma "Sharp Eyes" (Xueliang Gongcheng), finalizzato a estendere le capacità di sorveglianza anche alle aree rurali mediante l'integrazione delle telecamere pubbliche e private in un'unica rete di monitoraggio accessibile alle autorità locali. Secondo alcune stime, il numero di telecamere di sorveglianza presenti sul territorio cinese supera ormai diverse centinaia di milioni, rendendo tale infrastruttura una delle più capillari al mondo²¹⁹.

L'integrazione tra tali sistemi di videosorveglianza e tecnologie di riconoscimento facciale ha consentito lo sviluppo di sofisticati strumenti di identificazione automatica delle persone nello spazio pubblico. In particolare, i sistemi utilizzati in Cina operano

²¹⁷ Cfr. R. CREEMERS, *China's emerging data protection framework*, in *Journal of cybersecurity*, 2022, pag. 1 s.; cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 359, 366 ss.

²¹⁸ Cfr. Human Rights Watch, *China's algorithms of repression, reverse engineering a Xinjiang police mass surveillance app*, 2019, pag. 13 ss.; cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 350 s.; cfr. K. SHI-KUPFER, M. OHLBERG, *China's digital rise, challenges for Europe*, in *Merics papers on China*, n. 7, Aprile 2019, pag. 8 ss.

²¹⁹ Cfr. Human Rights Watch, *China's algorithms of repression, reverse engineering a Xinjiang police mass surveillance app*, 2019, pag. 13, da cui emerge chiaramente che l'espansione urbana è nota come Project Skynet, mentre quella relativa agli spazi rurali è nota come Project Sharp Eyes; cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 350

prevalentemente secondo modalità di identificazione one-to-many, che permettono di confrontare l'immagine del volto acquisita dalle telecamere con ampie banche dati biometriche contenenti milioni di profili individuali. Ciò consente alle autorità di sicurezza di effettuare operazioni di identificazione anche in tempo reale, rendendo possibile il monitoraggio dei movimenti delle persone nei principali spazi urbani, nei sistemi di trasporto e in molti contesti della vita quotidiana²²⁰. Secondo diversi studi accademici, l'adozione di tali tecnologie si inserisce in una più ampia strategia di modernizzazione delle capacità di controllo dello Stato, spesso descritta nella letteratura come un esempio di sorveglianza digitale²²¹.

Lo sviluppo dei sistemi di riconoscimento facciale in Cina è stato inoltre favorito dalla presenza di un settore tecnologico altamente competitivo, nel quale operano alcune tra le principali aziende mondiali specializzate nell'intelligenza artificiale applicata alla visione artificiale. Tra queste si possono ricordare società come Hikvision, Megvii (Face++) e SenseTime, che hanno sviluppato algoritmi avanzati di identificazione facciale utilizzati sia in ambito commerciale sia nei sistemi di sicurezza pubblica²²². L'ampia disponibilità di dati biometrici e l'estensione delle infrastrutture di videosorveglianza hanno così contribuito a creare un ecosistema tecnologico particolarmente favorevole allo sviluppo e all'implementazione su larga scala di tali strumenti.

Ulteriore elemento che contribuisce a comprendere il ruolo delle tecnologie di riconoscimento facciale nel contesto cinese, è il progressivo sviluppo di sistemi di governance digitale basati sulla raccolta e l'elaborazione di grandi quantità di dati relativi ai comportamenti individuali. In tale prospettiva, particolare attenzione è stata

²²⁰ Cfr. J. A. LEE, P. ZHOU, *FRT regulation in China*, in Cambridge University Press, pag. 242 ss.; cfr. R. CREEMERS, *China's emerging data protection framework*, in Journal of cybersecurity, 2022, pag. 242 s.; cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in International Journal of Law and Information Technology, vol. 31/2023, pag. 350 ss.; cfr. Human Rights Watch, *China's algorithms of repression, reverse engineering a Xinjiang police mass surveillance app*, 2019, pag. 1 ss., 13 ss.

²²¹ Cfr. J. A. LEE, P. ZHOU, *FRT regulation in China*, in Cambridge University Press, pag. 251 s.; cfr. V. N. GLISIN, S.M. MILASINOVIC, B. N. LECIC, *Artificial intelligence as a population surveillance tool: the case of China*, 2025, pag. 384 s.

²²² Cfr. J. A. LEE, P. ZHOU, *FRT regulation in China*, in Cambridge University Press, pag. 242 s.; cfr. T. NAITO, *Redefining the smart city for sustainable development*, in H. Kharas, J. Mcarthur, I. Ohno (a cura di), Breakthrough. The promise of frontier technologies for sustainable development, Brookings Institution Press, pag. 172; cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in International Journal of Law and Information Technology, vol. 31/2023, pag. 350

dedicata al cosiddetto Social Credit System, ovvero un complesso di iniziative normative e amministrative finalizzate alla valutazione dell'affidabilità economica e sociale di individui e imprese²²³. Sebbene tale sistema non costituisca un'unica piattaforma centralizzata, esso si fonda su una pluralità di programmi e banche dati che raccolgono informazioni relative ai comportamenti finanziari, amministrativi e sociali dei cittadini, allo scopo di incentivare comportamenti ritenuti conformi agli standard stabiliti dalle autorità pubbliche. Secondo alcuni studiosi, l'integrazione tra tali sistemi di valutazione e le tecnologie di sorveglianza digitale rappresenta uno degli aspetti più innovativi – e al tempo stesso controversi – del modello cinese di governance tecnologica, in quanto consente alle autorità di combinare strumenti di monitoraggio tecnologico con meccanismi di regolazione sociale²²⁴.

In questo contesto, le tecnologie di riconoscimento facciale assumono un ruolo particolarmente rilevante nell'ambito delle politiche di sicurezza urbana e nella gestione degli spazi pubblici. Negli ultimi anni, infatti, la Repubblica Popolare Cinese ha promosso numerosi programmi di “smart city” e “safe city”, volti a integrare sistemi di videosorveglianza, infrastrutture digitali e piattaforme di analisi dei dati al fine di migliorare l'efficienza amministrativa e rafforzare le capacità di prevenzione dei reati. Tali iniziative prevedono l'impiego di tecnologie di intelligenza artificiale per l'analisi automatizzata dei flussi video provenienti dalle telecamere di sorveglianza, consentendo l'identificazione dei soggetti presenti nello spazio pubblico e il tracciamento dei loro movimenti. Secondo diversi studi, l'integrazione tra reti di videosorveglianza e algoritmi di riconoscimento facciale costituisce uno degli elementi centrali delle politiche di sicurezza urbana promosse dalle autorità cinesi negli ultimi due decenni²²⁵.

²²³ Cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 350; cfr. V. N. GLISIN, S.M. MILASINOVIC, B. N. LECIC, *Artificial intelligence as a population surveillance tool: the case of China*, 2025, pag. 384

²²⁴ Cfr. K. SHI-KUPFER, M. OHLBERG, *China's digital rise, challenges for Europe*, in *Merics papers on China*, n. 7, Aprile 2019, pag. 25, 42; cfr. V. N. GLISIN, S.M. MILASINOVIC, B.N. LECIC, *Artificial intelligence as a population surveillance tool: the case of China*, 2025, pag. 384

²²⁵ Cfr. T. NAITO, *Redefining the smart city for sustainable development*, in H. Kharas, J. McArthur, I. Ohno (a cura di), *Breakthrough. The promise of frontier technologies for sustainable development*, Brookings Institution Press, pag. 169; cfr. S. C. GREITENS, *Dealing with demand for China's global surveillance exports*, in *Global China*, Aprile 2020, pag. 6; cfr. V.N. GLISIN, S.M. MILASINOVIC, B.N. LECIC, *Artificial intelligence as a population surveillance tool: the case of China*, 2025, pag. 384

L'impiego dei sistemi di identificazione biometrica si estende inoltre a numerosi ambiti della vita quotidiana, tra cui i trasporti pubblici, i servizi finanziari e l'accesso a edifici e infrastrutture. In molte città cinesi, ad esempio, le tecnologie di riconoscimento facciale vengono utilizzate nei sistemi ferroviari e metropolitani per verificare l'identità dei passeggeri o per automatizzare i controlli di sicurezza negli aeroporti. Analogamente, dei sistemi di pagamento digitale consentono di effettuare transazioni commerciali attraverso il riconoscimento del volto dell'utente, integrando tecnologie biometriche e piattaforme di pagamento elettronico sviluppate dalle principali aziende tecnologiche del Paese. Tale diffusione delle tecnologie biometriche nella vita quotidiana è stata resa possibile anche dalla forte integrazione tra settore pubblico e imprese private operanti nel campo dell'intelligenza artificiale e della visione artificiale²²⁶.

Particolare attenzione è stata inoltre dedicata nella letteratura all'utilizzo delle tecnologie di riconoscimento facciale nell'ambito delle politiche di sicurezza adottate nella regione autonoma dello Xinjiang, dove vive una significativa popolazione appartenente alla minoranza etnica uigura. Secondo numerosi rapporti di organizzazioni internazionali e studi accademici, le autorità cinesi avrebbero impiegato sistemi avanzati di sorveglianza digitale, inclusi strumenti di riconoscimento facciale e analisi algoritmica dei dati, al fine di monitorare in modo capillare la popolazione locale. Tali tecnologie sarebbero state integrate con banche dati biometriche e sistemi di analisi predittiva volti a individuare comportamenti considerati potenzialmente sospetti dalle autorità²²⁷.

²²⁶ Cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 350 ss.; cfr. J. A. LEE, P. ZHOU, *FRT regulation in China*, in Cambridge University Press, pag. 242 s.; cfr. T. NAITO, *Redefining the smart city for sustainable development*, in H. Kharas, J. McArthur, I. Ohno (a cura di), *Breakthrough. The promise of frontier technologies for sustainable development*, Brooking Institution Press, pag. 172, 242 s.

²²⁷ Cfr. United Nation Human Rights, office of the high commissioner, *OHCHR Assessment of human rights concerns in the Xinjiang Uyghur autonomous region, people's Republic of China*, 2022, pag. 30 ss.; cfr. Human Rights Watch, *China's algorithms of repression, reverse engineering a Xinjiang police mass surveillance app*, 2019, pag. 1 ss., 13 ss.

Questo tipo di utilizzo delle tecnologie biometriche ha suscitato un ampio dibattito nella comunità internazionale, sollevando interrogativi circa le implicazioni di tali strumenti per la tutela dei diritti fondamentali e delle libertà individuali²²⁸.

Nel complesso, l'esperienza analizzata mostra come i sistemi di riconoscimento facciale possano essere integrati all'interno di un modello di governance tecnologica fortemente centralizzato, nel quale le esigenze di sicurezza pubblica e di gestione amministrativa della società assumono un ruolo prioritario rispetto alla tutela della sfera privata degli individui. Proprio tale configurazione istituzionale rende il caso cinese particolarmente significativo nell'ambito dell'analisi comparata, poiché consente di mettere in evidenza le profonde differenze che intercorrono tra il modello europeo, fondato sulla centralità dei diritti fondamentali e sulla limitazione del potere pubblico, e sistemi nei quali le tecnologie di identificazione biometrica diventano parte integrante delle politiche statali di controllo e sicurezza. Proprio tali caratteristiche rendono il caso cinese uno dei riferimenti più rilevanti nel dibattito comparato sul rapporto tra innovazione tecnologica, sorveglianza e tutela dei diritti fondamentali, evidenziando al contempo le profonde differenze rispetto ai modelli normativi sviluppati negli ordinamenti europei²²⁹.

Alla luce di tutto ciò, il modello cinese di utilizzo delle tecnologie di riconoscimento facciale evidenzia una configurazione del rapporto tra innovazione tecnologica e tutela dei diritti individuali che è profondamente diversa da quella che si è sviluppata negli ordinamenti europei. In Unione europea l'impiego di sistemi biometrici è generalmente subordinato a un rigoroso bilanciamento tra esigenze di pubblica sicurezza e protezione dei diritti fondamentali, mentre nel contesto cinese queste tecnologie sono maggiormente integrate nelle strategie di governance statale e nelle politiche di sicurezza interna²³⁰.

²²⁸ Cfr. United Nation Human Rights, office of the high commissioner, *OHCHR Assessment of human rights concerns in the Xinjiang Uyghur autonomous region, people's Republic of China*, 2022, pag. 43 ss.; cfr. Human Rights Watch, *China's algorithms of repression, reverse engineering a Xinjiang police mass surveillance app*, 2019, pag. 1 ss., 50 ss.

²²⁹ Cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 359; cfr. J.A. LEE, P. ZHOU, *FRT regulation in China*, in Cambridge University Press, pag. 243, 251 s.; cfr. K. SHI-KUPFER, M. OHLBERG, *China's digital rise, challenges for Europe*, in *Merics papers on China*, n. 7, Aprile 2019, pag. 8 ss.

²³⁰ Cfr. R. ONG, *Privacy and personal information protection in China's all-seeing state*, in *International Journal of Law and Information Technology*, vol. 31/2023, pag. 359; cfr. K. SHI-KUPFER, M. OHLBERG,

L'analisi di questa esperienza comparata consente dunque di mettere in luce non solo le opportunità, ma anche i rischi connessi alla diffusione delle tecnologie biometriche su larga scala, mostrando come la regolazione giuridica di tali strumenti possa incidere in maniera significativa sull'equilibrio tra innovazione tecnologica, sicurezza pubblica e tutela dei diritti fondamentali. Proprio alla luce di tali considerazioni, risulta particolarmente interessante esaminare anche altri modelli internazionali di utilizzo delle tecnologie biometriche, nei quali il rapporto tra identificazione digitale e diritti individuali assume configurazioni ulteriormente differenti.

2. *Il sistema Aadhaar indiano: identità biometrica e accesso ai servizi*

Tra le esperienze internazionali più significative nell'ambito dell'impiego delle tecnologie biometriche, particolare rilievo assume il caso dell'India che, negli ultimi anni, ha sviluppato uno dei più vasti sistemi di identificazione digitale della popolazione del mondo²³¹. Il sistema Aadhaar non costituisce in senso stretto un sistema analogo a quelli impiegati per l'identificazione automatizzata nello spazio pubblico, ma assume rilievo in questa sede perché rappresenta una delle più ampie infrastrutture di identificazione biometrica della popolazione, fondata sulla raccolta e sull'uso di dati biometrici per finalità amministrative e di accesso ai servizi.

A differenza del modello cinese, caratterizzato da una forte integrazione tra tecnologie di sorveglianza e politiche di sicurezza statale, l'esperienza indiana si colloca all'interno di un contesto istituzionale formalmente democratico e costituzionalmente orientato alla tutela dei diritti fondamentali²³². Tuttavia, proprio la diffusione su ampia scala di sistemi di identificazione biometrica ha sollevato un ampio dibattito giuridico

China's digital rise, challenges for Europe, in Merics papers on China, n. 7, Aprile 2019, pag. 8 ss.; cfr. R. CREEMERS, *China's emerging data protection framework*, in Journal of cybersecurity, 2022, pag. 1 s.

²³¹ Cfr. Unique Identification Authority of India, *Annual report 2024-2025*, pag. 36, 61 s.; cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in Health Technol., 2017, pag. 5 s.

²³² Cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in Health Technol., Springer 2017, pag. 5 s.

e politico circa le implicazioni di tali strumenti per la protezione della privacy e delle libertà individuali²³³.

Dal punto di vista costituzionale, la Costituzione indiana del 1950 rappresenta uno dei testi fondamentali più articolati tra quelli adottati nel secondo dopoguerra: è previsto un catalogo di diritti fondamentali, tra cui la libertà personale, la libertà di espressione e il principio di eguaglianza dinanzi alla legge²³⁴. A lungo però, il diritto alla privacy non è stato espressamente riconosciuto come diritto fondamentale, e solo in tempi recenti la Corte Suprema indiana ha affermato la natura fondamentale di tale diritto²³⁵. In particolare, nella decisione *Justice K.S. Puttaswamy v. Union of India* del 2017, la Corte Suprema ha stabilito che il diritto alla privacy costituisce una componente essenziale del diritto alla libertà personale garantito dall'articolo 21 della Costituzione, riconoscendone la natura di diritto fondamentale opponibile allo Stato²³⁶.

Il riconoscimento costituzionale del diritto alla privacy ha assunto particolare rilievo nel contesto dello sviluppo delle politiche di digitalizzazione promosse dal governo indiano negli ultimi anni²³⁷. In tale ambito, il progetto più significativo è rappresentato dal sistema Aadhaar, un programma di identificazione biometrica lanciato nel 2009 con l'obiettivo di fornire a ogni residente indiano un numero di identificazione univoco basato sulla raccolta di dati biometrici, tra cui impronte digitali e scansioni dell'iride. Il sistema Aadhaar è gestito dalla Unique Identification Authority of India (UIDAI) e costituisce oggi la più grande banca dati biometrica esistente al mondo, coinvolgendo oltre un miliardo di persone²³⁸. Il funzionamento di tale sistema si basa sulla raccolta

²³³ Cfr. V. SINGH, *The Aadhaar verdict and the surveillance challenge*, Indian Journal of Law and Technology, vol. 15, issue 1, 2019, pag. 5 s., 13, 17; cfr. R. KHERA, *Impact of Aadhaar on welfare programmes*, in Economic & Political Weekly, vol. 52, n. 50, 2017, pag. 61 s.

²³⁴ V. Costituzione indiana, artt. 14, 19, 21

²³⁵ V. Supreme Court of India, 24 agosto 2017, *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1; cfr. A. PADMANABHAN, V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in Indian Journal of Law and Technology, vol. 15, issue 1, 2019, pag. 1 ss.

²³⁶ V. Supreme Court of India, 24 agosto 2017, *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1

²³⁷ Cfr. A. PADMANABHAN, V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in Indian Journal of Law and Technology, vol. 15, issue 1, 2019, pag. 11 s.; cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in Health Technol., Springer 2017, pag. 5 s.

²³⁸ Cfr. Unique Identification Authority of India, *Annual report 2024-2025*, pag. 16 s, 35 s., 61 s.; cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in Health Technol., Springer 2017, pag. 5 s.

e sull'archiviazione centralizzata di dati biometrici e demografici dei cittadini, ai quali viene attribuito un numero identificativo di dodici cifre²³⁹. Tale identificatore può essere utilizzato per accedere a una vasta gamma di servizi pubblici e privati, tra cui programmi di assistenza sociale, servizi bancari e sistemi di pagamento digitale²⁴⁰. Secondo i promotori del progetto, Aadhaar rappresenta uno strumento fondamentale per migliorare l'efficienza dell'amministrazione pubblica e ridurre fenomeni di frode o duplicazione nell'erogazione dei servizi sociali. Allo stesso tempo, tuttavia, la creazione di una banca dati biometrica di dimensioni così estese ha suscitato numerose preoccupazioni in relazione alla protezione dei dati personali e al rischio di sorveglianza digitale della popolazione²⁴¹.

Le questioni relative alla legittimità costituzionale del sistema Aadhaar sono state oggetto di un intenso contenzioso giudiziario culminato nella decisione della Corte Suprema indiana del 2018 (*Puttaswamy II*)²⁴². In tale occasione, la Corte ha riconosciuto la legittimità del sistema di identificazione biometrica come strumento finalizzato alla realizzazione di politiche di welfare e inclusione sociale, ma ha al tempo stesso imposto alcune limitazioni al suo utilizzo, stabilendo che l'impiego dell'identificatore Aadhaar dovesse essere circoscritto a specifiche finalità e non potesse essere imposto indiscriminatamente per l'accesso a servizi privati²⁴³. Tale pronuncia rappresenta uno dei più significativi esempi di intervento giurisprudenziale

²³⁹ Cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health Technol.*, Springer 2017, pag. 9; cfr. Unique Identification Authority of India, *Annual report 2024-2025*, pag. 17, 35 s.

²⁴⁰ Cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health Technol.*, Springer 2017, pag. 5, 9 s.; cfr. Unique Identification Authority of India, *Annual report 2024-2025*, pag. 17, 52

²⁴¹ Cfr. Unique Identification Authority of India, *Annual report 2024-2025*, pag. 17, 52; cfr. A. PADMANABHAN, V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in *Indian Journal of Law and Technology*, vol. 15, issue 1, 2019, pag. 12 ss., 17 ss.; cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health Technol.*, Springer 2017, pag. 9

²⁴² V. Supreme Court of India, sent. 26 settembre 2018, *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, Writ Petition (Civil) No. 494 of 2012, (2019) 1 SCC 1; cfr. A. PADMANABHAN, V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in *Indian Journal of Law and Technology*, vol. 15, issue 1, 2019, pag. 12 s.

²⁴³ V. Supreme Court of India, sent. 26 settembre 2018, *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, Writ Petition (Civil) No. 494 of 2012, (2019) 1 SCC 1, nelle parti in cui la Corte valorizza il Sistema Aadhaar come strumento per "targeted delivery of subsidies, benefits and services" nonchè per l'inclusione dei soggetti più vulnerabili; cfr. A. PADMANABHAN, V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in *Indian Journal of Law and Technology*, vol. 15, issue 1, 2019, pag. 12 ss., 17 ss.

volto a bilanciare le esigenze di innovazione tecnologica e di efficienza amministrativa con la tutela dei diritti fondamentali dei cittadini²⁴⁴.

Parallelamente allo sviluppo del sistema Aadhaar, l'India ha avviato negli ultimi anni un processo di riforma della normativa relativa alla protezione dei dati personali²⁴⁵. In particolare, nel 2023 il legislatore indiano ha adottato il Digital Personal Data Protection Act, una legge volta a disciplinare il trattamento dei dati personali e a introdurre specifiche garanzie per la tutela della privacy degli individui. Tale normativa rappresenta il primo tentativo organico di regolazione del trattamento dei dati personali nell'ordinamento indiano e si inserisce in un più ampio processo di adeguamento del sistema giuridico nazionale agli standard internazionali in materia di protezione dei dati²⁴⁶.

Nonostante tali sviluppi normativi, il sistema di identificazione biometrica indiano continua a sollevare numerosi interrogativi sotto il profilo della tutela dei diritti fondamentali. Diversi studiosi hanno evidenziato come la centralizzazione di grandi quantità di dati biometrici possa comportare rischi significativi in termini di sicurezza informatica, utilizzo improprio delle informazioni personali e potenziale estensione delle capacità di monitoraggio dello Stato²⁴⁷. Allo stesso tempo, il sistema Aadhaar è stato oggetto di critiche anche sotto il profilo dell'inclusione sociale, in quanto eventuali errori nei sistemi biometrici o difficoltà tecniche nel processo di

²⁴⁴ Cfr. A. PADMANABHAN, V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in Indian Journal of Law and Technology, vol. 15, issue 1, 2019, pag. 12 ss.; cfr. V. BHANDARI, K. LAHIRI, *The surveillance State, privacy and criminal investigation in India: possible futures in a post-Puttaswamy world*, in University of Oxford Human Rights Hub Journal, vol. 3(2), 2020, pag. 29 s.

²⁴⁵ V. The digital Personal Data Protection Act, n. 22 del 2023; cfr. G. GREENLEAF, *Global Data Privacy Laws 2023: 162 national laws and 20 bills*, in UNSW Law Research Paper n. 23-48, 2023 pag. 2 ss.

²⁴⁶ V. The digital Personal Data Protection Act, 2023, n. 22., 11 August 2023, sec. 1; cfr. G. GREENLEAF, *Global Data Privacy Laws 2023: 162 national laws and 20 bills*, in in UNSW Law Research Paper n. 23-48, 2023, pag. 2 ss.; cfr. R. YADAV, R. VARSHNEY, *Recalibrating the right to privacy in the digital age: legal challenges and constitutional safeguards in the era of technological intrusion*, in ShodhKosh: journal of visual and performing arts, 2024, pag. 1958 ss.

²⁴⁷ Cfr. A. PADMANABHAN, V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in Indian Journal of Law and Technology, vol. 15, issue 1, 2019, pag. 12 ss., 17 s.; cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in Health Technol., Springer 2017, pag. 5 ss., 7 ss., 20

autenticazione possono comportare l'esclusione di alcuni individui dall'accesso a servizi essenziali²⁴⁸.

Nel complesso, l'esperienza indiana evidenzia un modello di utilizzo delle tecnologie biometriche significativamente diverso sia dal sistema europeo sia da quello cinese. Se da un lato l'ordinamento indiano riconosce formalmente il diritto alla privacy come diritto fondamentale e prevede un sistema di controllo giurisdizionale sulle politiche pubbliche²⁴⁹, dall'altro la diffusione di sistemi di identificazione biometrica su scala nazionale dimostra come le tecnologie digitali possano essere impiegate anche in contesti democratici per finalità di gestione amministrativa e di inclusione sociale²⁵⁰. Proprio tale ambivalenza rende il caso indiano particolarmente interessante nell'ambito dell'analisi comparata delle tecnologie di identificazione biometrica, poiché esso mostra come l'uso di tali strumenti possa essere giustificato non soltanto in funzione della sicurezza pubblica, ma anche come strumento di modernizzazione dell'amministrazione e di ampliamento dell'accesso ai servizi pubblici.

Alla luce di quanto osservato, l'esperienza indiana mostra come l'impiego delle tecnologie biometriche possa assumere caratteristiche peculiari anche all'interno di ordinamenti democratici dotati di un sistema costituzionale orientato alla tutela dei diritti fondamentali. A differenza del modello cinese, nel quale l'utilizzo delle tecnologie di identificazione facciale appare strettamente connesso alle politiche di sicurezza e controllo sociale promosse dallo Stato, il sistema indiano si sviluppa principalmente nell'ambito delle politiche di digitalizzazione dell'amministrazione e di ampliamento dell'accesso ai servizi pubblici. Ciò nonostante, la creazione di una banca dati biometrica di dimensioni senza precedenti come quella prevista dal sistema Aadhaar ha sollevato numerose questioni relative alla protezione della privacy, alla sicurezza dei dati personali e al rischio di un utilizzo estensivo delle tecnologie di

²⁴⁸ Cfr. R. KHERA, *Impact of Aadhaar programmes*, in *Economic & political Weekly*, vol. 52, n. 50, 2017, pag. 61 ss.; cfr. U. JAIN, *Right to privacy and the Aadhaar Act: a critical study*, in *Bharati Law Review*, Dicembre 2018, pag. 175 ss., 181

²⁴⁹ V. Supreme Court of India, sent. 24 agosto 2017, *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1; cfr. V. BHANDARI, K. LAHIRI, *The surveillance State, privacy and criminal investigation in India: possible futures in a post-Puttaswamy world*, in *University of Oxford Human Rights Hub Journal*, vol. 3(2), 2020, pag. 29 s.

²⁵⁰ Cfr. Unique Identification Authority of India, *Annual report 2024-2025*, pag. 17, 52; cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health Technol.*, Springer 2017, pag. 5 s.

identificazione digitale da parte delle autorità pubbliche²⁵¹. Il dibattito giuridico sviluppatosi attorno alle decisioni della Corte Suprema indiana dimostra come anche nei sistemi democratici l'introduzione di strumenti biometrici su larga scala richieda un costante bilanciamento tra esigenze di efficienza amministrativa, innovazione tecnologica e tutela dei diritti fondamentali della persona²⁵².

Per tali ragioni, il caso indiano rappresenta un ulteriore e significativo punto di osservazione nell'ambito dell'analisi comparata delle tecnologie di identificazione biometrica. Esso consente infatti di evidenziare come tali strumenti possano essere impiegati non solo per finalità di sicurezza pubblica, ma anche come strumenti di identificazione digitale della popolazione e di gestione dei servizi pubblici, aprendo al contempo nuovi interrogativi circa le implicazioni di tali sistemi per la tutela della privacy e delle libertà individuali.

3. *Giamaica e Kenya: identità digitale nazionale e biometria amministrativa*

Le esperienze giamaicana e kenyota assumono rilievo comparato non tanto perché riproducono i modelli di riconoscimento facciale nello spazio pubblico analoghi a quelli esaminati con riguardo alla Cina o, come avremo modo di vedere nel proseguo, alla Russia, quanto piuttosto perché mostrano una diversa modalità di espansione delle tecnologie biometriche nell'azione pubblica. Il loro interesse, quindi, non risiede nell'uso del riconoscimento facciale come tecnica di sorveglianza urbana in senso stretto, ma nella costruzione di sistemi pubblici di identificazione digitale fondati sulla raccolta e sull'uso dei dati biometrici. In entrambi gli ordinamenti, infatti, l'identificazione biometrica è presentata come uno strumento di modernizzazione amministrativa, di contrasto alle frodi, di razionalizzazione della spesa pubblica e di più efficiente accesso ai servizi essenziali. Proprio tali finalità, apparentemente orientate all'inclusione e alla semplificazione, rendono tali vicende paradigmatiche in quanto mostrano come l'impiego dei dati biometrici da parte dello Stato possa incidere

²⁵¹ Cfr. A. PADMANABHAN, V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in Indian Journal of Law and Technology, vol. 15, issue 1, 2019, pag. 13, 17 s.; cfr. P. DIXON, *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in Health Technol., Springer 2017, pag. 7, 9, 20

²⁵² Cfr. A. PADMANABHAN, V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in Indian Journal of Law and Technology, vol. 15, issue 1, 2019, pag. 12 ss.; cfr. V. BHANDARI, K. LAHIRI, *The surveillance State, privacy and criminal investigation in India: possible futures in a post-Puttaswamy world*, in University of Oxford Human Rights Hub Journal, vol. 3(2), 2020, pag. 29 s.

sui diritti fondamentali non solo quando assume la forma della sorveglianza, ma anche quando viene inserito nelle infrastrutture amministrative destinate a regolare l'accesso ai diritti sociali. In questa prospettiva, questi casi si pongono in continuità con l'esperienza indiana perché confermano che la trasformazione dell'identità individuale in dato biometrico centralizzato tende a sbilanciare il rapporto tra l'efficienza pubblica e le garanzie costituzionali della persona²⁵³.

In Giamaica, il progetto di National Identification System (c.d. NIS) era stato costruito attorno all'idea di un'identità digitale nazionale univoca, funzionale a semplificare i rapporti tra cittadini e amministrazione pubblica e a ridurre i fenomeni di frode, corruzione e dispersione delle risorse pubbliche. La scelta di fondare tale sistema sulla raccolta centralizzata di dati personali e biometrici, unitamente al carattere sostanzialmente invasivo del meccanismo di registrazione e verifica, tuttavia, ha posto il problema della sua compatibilità con il quadro costituzionale dei diritti²⁵⁴. La Charter of Fundamental Rights and Freedoms della Costituzione giamaicana del 1962 tutela, infatti, sia il rispetto e la protezione della vita privata e familiare, sia la privacy domestica e delle comunicazioni²⁵⁵. Su tale base, nella decisione *Julian J. Robinson v. The Attorney General of Jamaica* del 2019, la Corte Suprema ha ritenuto che una parte essenziale dell'impianto normativo fosse sproporzionata rispetto agli obiettivi perseguiti e ha sottolineato che l'invasività del sistema non si poteva giustificare solo mediante generici richiami all'efficienza amministrativa, alla lotta ai reati o ai benefici economici attesi. Significativa è l'idea, che sta alla base della pronuncia, per cui la costituzionalità del sistema non si possa valutare sulla base di garanzie future o mere promesse, ma si debba misurare alla luce del quadro normativo effettivamente

²⁵³ Cfr. G. FORMICI, *Digital Welfare State and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *Federalismi* (www.federalismi.it), n. 26/2022, pag. 1 s., 6 s.; cfr. F. BAILO, *Welfare digitale: opportunità e prospettive dal diritto costituzionale*, in L. Troiani (a cura di), *Politiche del welfare e costituzionalismo europeo. Il rapporto Beveridge ottant'anni dopo*, 2023, pag. 169 s.

²⁵⁴ Cfr. G. FORMICI, *Digital Welfare State and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *Federalismi* (www.federalismi.it), n. 26/2022, pag. 13 ss.; cfr. H.S. DUNN, *Risking identity: a case study of Jamaica's short-lived national ID system*, in *Journal of Information, Communication and Ethics in Society*, vol. 18, n. 3, 2020, pag. 329 ss.

²⁵⁵ V. Charter of Fundamental Rights and Freedoms Act (Constitutional Amendment), 2011, sec. 13 (3) (j) (ii) s., sec. 13 (3) (g) ss.; cfr. G. FORMICI, *Digital Welfare State and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *Federalismi* (www.federalismi.it), n. 26/2022, pag. 14; cfr. H. S. DUNN, *Risking identity: a case study of Jamaica's short-lived national ID system*, in *Journal of Information, Communication and Ethics in Society*, vol. 18, n. 3, 2020, pag. 330

esistente al momento dell'introduzione del trattamento. Da tale pronuncia emerge una concezione di privacy che non può essere ridotta a mera segretezza, ma che deve essere letta come presidio dell'autonomia individuale, della dignità e della libertà di autodeterminazione rispetto alla raccolta e circolazione di informazioni personali²⁵⁶.

La vicenda giamaicana, inoltre, mostra come, in materia di identificazione biometrica, il problema non si esaurisca nella sola esistenza di una finalità pubblica legittima. La Corte, infatti, non ha negato in assoluto che lo Stato possa perseguire obiettivi di migliore identificazione della popolazione o di più ordinata gestione dei servizi, ma ha rilevato che tali finalità devono essere perseguite con strumenti conformi al principio di proporzionalità e accompagnati da effettive garanzie contro eventuali accessi indebiti, usi secondari dei dati e possibili derive verso forme di controllo generalizzato²⁵⁷. Non è casuale che nel dibattito successivo sia riemersa l'esigenza di un sistema volontario, quindi, meno invasivo e inserito in una cornice robusta di protezione dei dati personali: proprio a tal fine è stato adottato il National Identification and Registration Act nel 2021, ed è stato contestualmente valorizzato il Data Protection Act del 2020. Sul piano del dibattito pubblico e della riflessione giuridica interna, inoltre, il caso è stato letto come indice di una più ampia crisi fiduciaria verso le infrastrutture identitarie centralizzate che non siano accompagnate da trasparenza, consultazione pubblica e adeguate salvaguardie²⁵⁸.

Il Kenya, poi, presenta tratti analoghi, ma mette in luce con maggiore evidenza il nesso tra l'identificazione biometrica, l'uguaglianza sostanziale e il rischio di esclusione. Con l'introduzione del National Integrated Identity Management System (c.d. Huduma

²⁵⁶ Cfr. Supreme Court of Judicature of Jamaica, Full Court, sent. 12 aprile 2019, *Julian J. Robinson v. The Attorney General of Jamaica*, Claim No. 2018HCV01788, [2019] JMFC Full 04; cfr. G. FORMICI, *Digital Welfare State and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *Federalismi* (www.federalismi.it), n. 26/2022, pag. 14 s.; cfr. H. S. DUNN, *Risking identity: a case study of Jamaica's short-lived national ID system*, in *Journal of Information, Communication and Ethics in Society*, vol. 18, n. 3, 2020, pag. 334 s.

²⁵⁷ Cfr. G. FORMICI, *Digital Welfare State and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *Federalismi* (www.federalismi.it), n. 26/2022, pag. 14 s.; cfr. H. S. DUNN, *Risking identity: a case study of Jamaica's short-lived national ID system*, in *Journal of Information, Communication and Ethics in Society*, vol. 18, n. 3, 2020, pag. 333 ss.

²⁵⁸ Cfr. F. BAILO, *Welfare digitale: opportunità e prospettive dal diritto costituzionale*, in L. Troiani (a cura di), *Politiche del welfare e costituzionalismo europeo. Il rapporto Beveridge ottant'anni dopo*, 2023, pag. 177; cfr. H. S. DUNN, *Risking identity: a case study of Jamaica's short-lived national ID system*, in *Journal of Information, Communication and Ethics in Society*, vol. 18, n. 3, 2020, pag. 329 s.

Namba) il legislatore ha creato un'infrastruttura unitaria di identificazione della popolazione fondata sulla raccolta e il trattamento di un insieme estremamente ampio di dati, inclusi quelli biometrici e – in origine – il DNA e le coordinate GPS²⁵⁹. La questione si colloca immediatamente entro il perimetro della Costituzione kenyota del 2010, la quale riconosce espressamente il diritto alla privacy, ma anche i principi di eguaglianza e di non discriminazione. In particolare, l'articolo 31 protegge la persona da interferenze arbitrarie nella sfera privata e dalle indebite intrusioni nelle informazioni sulla sua vita, mentre l'articolo 27 vieta discriminazioni dirette e indirette e impone di garantire eguale protezione ed eguale beneficio della legge. Proprio questo intreccio tra privacy ed eguaglianza permette di capire perché il contenzioso su Huduma Namba abbia assunto sin da subito una portata costituzionale tanto ampia²⁶⁰.

Nella decisione *Nubian Rights Forum v. Attorney General* del 2020, la High Court di Nairobi non ha escluso astrattamente la possibilità per lo Stato di dotarsi di un sistema nazionale di identificazione digitale, ma ha chiarito che un simile progetto può essere legittimato solo se limitato. La Corte, anzitutto, ha rilevato che la raccolta di dati come DNA e coordinate GPS ha un grado di intrusività incompatibile con il diritto alla privacy se manca una base normativa specifica, precisa e adeguatamente garantita e per questa ragione ne ha affermato l'incostituzionalità. Nella stessa pronuncia, la Corte ha sottolineato che l'implementazione del sistema non poteva procedere senza un quadro normativo sufficientemente completo in materia di protezione dei dati personali: sarebbe stato più conforme alla Costituzione approntare prima tale quadro, e solo successivamente dare corso alla raccolta e al trattamento massivo delle informazioni personali. D'altra parte, è stata evidenziata la possibilità che il nuovo sistema identitario producesse effetti discriminatori nei confronti di gruppi già vulnerabili – quali la comunità nubiana e i soggetti che incontrano ostacoli documentali o amministrativi in sede di accesso ai registri civili e ai servizi pubblici.

²⁵⁹ Cfr. F. BAILO, *Welfare digitale: opportunità e prospettive dal diritto costituzionale*, in L. Troiani (a cura di), *Politiche del welfare e costituzionalismo europeo. Il rapporto Beveridge ottant'anni dopo*, 2023, pag. 177 s.; cfr. G. FORMICI, *Digital Welfare State and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *Federalismi* (www.federalismi.it), n. 26/2022, pag. 18 s.; cfr. N. KIILU, *Indirect Discrimination: Huduma Namba (Digital Identification) and the Plight of the Nubian Community in Kenya*, *Strathmore Law Review*, vol. 7, issue 1, 2022, pag. 22 s.

²⁶⁰ V. Costituzione kenyota, artt. 27 e 31; cfr. N. KIILU, *Indirect Discrimination: Huduma Namba (Digital Identification) and the Plight of the Nubian Community in Kenya*, *Strathmore Law Review*, vol. 7, issue 1, 2022, pag. 27 ss, 37 ss.

In questo modo il problema legato alla biometria non viene più colto solo nella sua dimensione della riservatezza, ma anche nella sua dimensione di meccanismo di riproduzione istituzionale delle diseguaglianze²⁶¹.

L'esperienza del Kenya consente, quindi, di mettere a fuoco un punto tecnico chiave: quando l'identificazione digitale diventa presupposto per l'accesso a prestazioni o servizi essenziali, l'errore tecnologico o l'opacità delle procedure non incidono solo sul diritto alla protezione dei dati, ma possono tradursi in fattori di esclusione civica e sociale. Parte della dottrina locale ha insistito proprio su questo aspetto e ha sottolineato come sistemi apparentemente neutri possano produrre discriminazioni indirette e colpire gruppi che, storicamente, sono stati marginalizzati. L'identità biometrica, in questo senso, non è più da vedere come mero strumento tecnico di registrazione in quanto diventa un'infrastruttura giuridica capace di ridefinire in concreto il rapporto tra individui e Stato, sino al punto di condizionare l'effettività dei diritti fondamentali²⁶².

I casi in esame, se letti congiuntamente, mostrano che il problema giuridico delle tecnologie biometriche non coincide solo con il rischio di sorveglianza nello spazio pubblico, ma investe anche la progressiva trasformazione dell'identità personale in chiave di accesso ai diritti. Se nei modelli securitari le criticità sono legate al controllo e al monitoraggio diffuso, nei sistemi di welfare digitale la tensione si manifesta ove l'identificazione biometrica diviene condizione per essere riconosciuti dall'amministrazione e per accedere a prestazioni, documenti e servizi. Proprio per questo tali esperienze sono preziose nell'ambito di una ricerca dedicata ai sistemi di riconoscimento facciale e al loro impatto sui diritti fondamentali e mostrano che la logica biometrica, anche al di fuori del riconoscimento facciale in tempo reale, può generare effetti profondi su vita privata, dignità, eguaglianza e inclusione sociale. Ne deriva che la valutazione giuridica di tali tecnologie non può arrestarsi al tema della

²⁶¹ Cfr. G. FORMICI, *Digital Welfare State and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *Federalismi* (www.federalismi.it), n. 26/2022, pag. 20 s.; cfr. N. KIILU, *Indirect Discrimination: Huduma Namba (Digital Identification) and the Plight of the Nubian Community in Kenya*, *Strathmore Law Review*, vol. 7, issue 1, 2022, pag. 22 s., 37 ss.

²⁶² Cfr. G. FORMICI, *Digital Welfare State and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *Federalismi* (www.federalismi.it), n. 26/2022, pag. 20; cfr. N. KIILU, *Indirect Discrimination: Huduma Namba (Digital Identification) and the Plight of the Nubian Community in Kenya*, *Strathmore Law Review*, vol. 7, issue 1, 2022, pag. 19 ss., 37 ss., 47

sicurezza o a quello dell'efficienza ma deve interrogarsi radicalmente sulle condizioni costituzionali entro cui la persona e i suoi dati possono essere trasformati in uno strumento ordinario di governo²⁶³.

4. *Il modello “innovativo” americano*

Nel panorama comparato relativo all'impiego delle tecnologie di riconoscimento facciale, il caso degli Stati Uniti presenta caratteristiche significativamente diverse sia rispetto ai modelli di sorveglianza centralizzati, sia rispetto ai sistemi di identificazione biometrica costruiti su basi pubblicistiche unitarie. L'esperienza statunitense, infatti, non si caratterizza per l'esistenza di un unico sistema nazionale di riconoscimento facciale, bensì per la presenza di una pluralità di strumenti e pratiche distribuite su più livelli: federale, statale, locale e privato. Proprio tale struttura costituisce uno dei tratti distintivi del modello americano: negli Stati Uniti, il riconoscimento facciale, si sviluppa come tecnologia dell'innovazione privata, poi incorporata anche nelle attività di law enforcement, nel controllo delle frontiere e nei servizi di identificazione commerciale. In questo contesto, il dibattito giuridico non si è concentrato tanto sull'esistenza di un apparato pubblico unitario, quanto piuttosto sulla difficoltà di ricondurre usi molteplici e frammentati entro un quadro normativo coerente²⁶⁴.

Dal punto di vista costituzionale, le questioni poste dal riconoscimento facciale si collocano all'incrocio tra diverse garanzie fondamentali. In primo luogo, viene in rilievo il quarto emendamento, che tutela i cittadini contro perquisizioni e sequestri irragionevoli e costituisce il parametro costituzionale principale rispetto alle nuove forme di sorveglianza tecnologica. In secondo luogo, assumono rilievo le libertà protette dal quinto emendamento, in particolare la libertà di espressione, di riunione e di associazione, nella misura in cui l'identificazione automatizzata nello spazio pubblico può produrre effetti dissuasivi sulla partecipazione a manifestazione, proteste

²⁶³ Cfr. G. FORMICI, *Digital Welfare State and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *Federalismi* (www.federalismi.it), n. 26/2022, pag. 28; cfr. F. BAILO, *Welfare digitale: opportunità e prospettive dal diritto costituzionale*, in L. Troiani (a cura di), *Politiche del welfare e costituzionalismo europeo. Il rapporto Beveridge ottant'anni dopo*, 2023, pag. 177.

²⁶⁴ Cfr. U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, GAO-23-105607, 2023, pag. 1 s., 12 ss.; cfr. D. LEVIN, *Face the facts, or is the face a fact?: biometric privacy in publicly available data*, in *Fordham Intellectual Property, Media and Entertainment Law Journal*, vol. 32, n. 4, 2022, pag. 1032 ss., spec. 1040 ss., 1063 s.

o altre forme di espressione politica. Sullo sfondo emergono poi i profili di cui al quattordicesimo emendamento, soprattutto con riguardo all'eguale protezione, in quanto l'accuratezza differenziale degli algoritmi rispetto a gruppi demografici diversi può tradursi in effetti discriminatori. La giurisprudenza costituzionale americana non ha, tuttavia, ancora elaborato una dottrina unitaria dedicata al riconoscimento facciale. Ciò nonostante, decisioni come *Carpenter v. United States* mostrano come la Corte Suprema abbia riconosciuto, progressivamente, la necessità di adattare le garanzie del quarto emendamento alle tecnologie capaci di consentire un monitoraggio pervasivo e prolungato dei movimenti individuali²⁶⁵.

Gli Stati Uniti, ad oggi, non conoscono una disciplina federale organica dei dati biometrici e del riconoscimento facciale. Ciò ha favorito uno sviluppo normativo fortemente disomogeneo in cui coesistono, da un lato, pratiche federali di impiego della tecnologia da parte delle autorità pubbliche e, dall'altro, discipline statali e locali più restrittive²⁶⁶. Sul piano federale, il Federal Bureau of Investigation gestisce il Next Generation Identification – Interstate Photo System (c.d. NGI-IPS) che offre alle autorità abilitate una funzione di ricerca tramite riconoscimento facciale su un archivio di oltre trenta milioni di foto segnaletiche criminali, pertanto è qualificabile come strumento investigativo. Parallelamente, l'agenzia investigativa indipendente del Congresso americano ha rilevato che diverse agenzie federali appartenenti al Dipartimento dell'Homeland Security e di Giustizia hanno utilizzato, per scopi investigativi, anche servizi di riconoscimento facciale forniti da soggetti privati capaci di operare ricerche su basi fotografiche estremamente ampie, in alcuni casi costituite da miliardi di immagini. In tal senso, il modello statunitense mostra con evidenza come

²⁶⁵ V. Costituzione statunitense, IV, V, XIV amendments, Section I; v. *Katz v. Supreme Court of the United States*, sent. 18 dicembre 1967, *Katz v. United States*, 389 U.S. 347 (1967); v. Supreme Court of the United States, sent. 22 giugno 2018, *Carpenter v. United States*, 138 S. Ct. 2206 (2018); cfr. O.S. KERR, *Four models of Fourth Amendment protection*, in Stanford Law Review, vol. 60, n. 2, pag. 504 ss.

²⁶⁶ Cfr. U.S. Government Accountability Office, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522, 2020, pag. 2, 42; cfr. U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, GAO-23-105607, 2023, pag. 1 s.

il confine tra infrastrutture pubbliche e risorse private risulti più poroso di quanto accada in altri ordinamenti²⁶⁷.

L'impiego del riconoscimento facciale negli Stati Uniti si è poi esteso in modo significativo anche ai controlli di frontiera e alla gestione dei flussi di viaggio. La U.S. Customs and Border Protection impiega sistemi di comparazione biometrica per verificare l'identità dei viaggiatori in diversi contesti di ingresso e uscita dal territorio, presentando tale tecnologia come strumento utile a rafforzare la sicurezza e a rendere più rapida l'identificazione. Si tratta di un ambito rilevante poiché mostra come il riconoscimento facciale non sia impiegato solo nella dimensione repressiva, ma anche in quella amministrativa e preventiva all'interno di procedure ordinarie di controllo della mobilità. La diffusione della biometria facciale si è qui realizzata non tramite una disciplina generale preventiva, ma tramite l'espansione progressiva di usi settoriali giustificati da esigenze di efficienza, sicurezza o semplificazione dei controlli²⁶⁸.

Ulteriore tratto distintivo del modello in esame è dato dal ruolo fondamentale che ha il settore privato: il riconoscimento facciale, infatti, è stato impiegato in una pluralità di contesti commerciali come la sicurezza privata, il controllo degli accessi, il retail, l'autenticazione, il marketing e i servizi digitali. Proprio in relazione al settore commerciale, il Government Accountability Office – c.d. GAO – ha evidenziato che la tecnologia è stata impiegata da imprese e che permangono rilevanti criticità tanto in materia di privacy, quanto con riferimento all'accuratezza dei sistemi e alla loro variabile affidabilità rispetto a gruppi demografici distinti. In questo contesto, il caso Clearview AI ha assunto grande valore in quanto ha dimostrato come un'impresa privata potesse costruire – tramite scraping massivo – un database biometrico di dimensioni eccezionali e renderlo poi disponibile alle autorità pubbliche. La vicenda ha reso evidente che, nel modello americano, il rischio per i diritti fondamentali non

²⁶⁷ V. Federal Bureau of Investigation, *Next Generation Identification (NGI)*; cfr. U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, GAO-23-105607, 2023, pag. 2, 12 ss.

²⁶⁸ V. U.S. Customs and Border Protection, *Biometrics Privacy Policy*; cfr. U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, GAO-23-105607, 2023, pag. 6, 12 ss.

deriva solo dall'uso pubblico della tecnologia, ma anche dalla disponibilità privata di grandi archivi biometrici suscettibili di successiva circolazione istituzionale²⁶⁹.

Accanto al caso Clearview AI, un ulteriore episodio significativo è rappresentato dalla vicenda di Robert Williams, un cittadino afroamericano arrestato nel 2020 a Detroit in seguito a una falsa corrispondenza prodotta da un sistema di riconoscimento facciale. Il caso è particolarmente rilevante in quanto consente di cogliere il rischio che l'output algoritmico, nato come elemento di orientamento investigativo, venga progressivamente assunto dall'autorità di polizia come determinante dell'identificazione del sospettato. Il problema, pertanto, non riguarda solo l'errore tecnico del sistema, ma il modo in cui tale errore viene recepito dall'apparato investigativo e tradotto in attività restrittive della libertà personale²⁷⁰.

La vicenda si inserisce nel più ampio dibattito sui falsi positivi e sui bias dei sistemi biometrici. Come già evidenziato, l'accuratezza dei sistemi di riconoscimento facciale dipende da molteplici fattori, tra cui la qualità dell'immagine, le condizioni di acquisizione, la rappresentatività del dataset e il contesto sociotecnico nel quale l'algoritmo viene sviluppato e utilizzato. Proprio per questo, quando tali strumenti sono impiegati dalle forze di polizia, il falso positivo non resta confinato al piano informatico, ma può trasformarsi in un errore istituzionale, esponendo il soggetto erroneamente identificato al rischio di controlli, interrogatori o arresti ingiustificati²⁷¹. Il caso Williams si è concluso nel 2024 con un accordo transattivo tra l'interessato e la città di Detroit, che ha anche imposto limiti più stringenti all'uso del riconoscimento facciale da parte del dipartimento di polizia. In particolare, l'accordo richiede che i risultati

²⁶⁹ Cfr. U.S. Government Accountability Office, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522, 2020, pag. 2, 8 ss., 42; cfr. D. LEVIN, *Face the facts, or is the face a fact?: biometric privacy in publicly available data*, in *Fordham Intellectual Property, Media and Entertainment Law Journal*, vol. 32, n. 4, 2022, pag. 1040 ss.; cfr. W. HARTZOG, *BIPA: the most important biometric privacy law in the US?*, in A. Kak (a cura di), *Regulating Biometrics: Global Approaches and Urgent Questions*, 2020, pag. 96 s.

²⁷⁰ Cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 183; cfr. K. HILL, *Wrongfully Accused by an Algorithm*, in *The New York Times*, 24 giugno 2020.

²⁷¹ Cfr. A. MASCOLO, *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in M. Macchia (a cura di) *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Giappichelli, 2026, pag. 183 s.; cfr. J. BUOLAMWINI, T. GEBRU, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning Research*, vol. 81, 2018, pag. 1 ss.; cfr. P. GROTH, M. NGAN, K. HANAOKA, *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects*, NIST Interagency Report 8280, 2019.

prodotti dalla tecnologia siano corroborati da elementi indipendenti e affidabili prima di procedere a un arresto, inoltre vieta la costruzione di lineup fotografiche fondate esclusivamente su un facial recognition lead. La vicenda, quindi, non determina un mutamento complessivo dell'ordinamento statunitense, ma assume valore paradigmatico: mostra come le garanzie contro l'uso distorto del riconoscimento facciale tendano a essere costruite in modo frammentario, spesso attraverso contenziosi, settlement e policies locali²⁷².

L'assenza di una disciplina federale unitaria ha favorito lo sviluppo di soluzioni normative molto diverse a livello statale. Uno degli esempi più significativi è rappresentato dallo Stato dell'Illinois, che con il Biometric Information Privacy Act ha introdotto una delle discipline più note e incisive in materia di dati biometrici, richiedendo informazione preventiva, consenso e limiti alla raccolta, conservazione e diffusione di dati biometrici. Accanto a tali scelte statali, non sono mancati interventi restrittivi anche a livello locale: la città di San Francisco è stata tra le prime ad adottare un divieto dell'uso delle tecnologie di riconoscimento facciale da parte delle autorità municipali, esprimendo in modo particolarmente netto la preoccupazione per gli effetti della tecnologia sul diritto alla privacy e sulle libertà civili. La stessa esperienza americana mostra, dunque, come il riconoscimento facciale sia divenuto terreno di una regolazione frammentata, in cui a usi estensivi in alcuni contesti si contrappongono moratorie, divieti o discipline più rigorose in altri²⁷³.

Le criticità di tale modello emergono con particolare chiarezza proprio alla luce dei diritti fondamentali coinvolti. Da un lato, la possibilità di identificare automaticamente individui nello spazio pubblico o in contesti commerciali rischia di comprimere la sfera della vita privata e di erodere l'anonimato che tradizionalmente accompagna la circolazione negli spazi aperti al pubblico. Dall'altro lato, l'uso del riconoscimento

²⁷² Cfr. *Settlement Agreement, Williams v. City of Detroit*, United States District Court for the Eastern District of Michigan, Southern Division, Case No. 2:21-cv-10827, 28 giugno 2024; ACLU, *Williams v. City of Detroit*, 28 giugno 2024; ACLU Michigan, *Facial Recognition*, 2024

²⁷³ V. Illinois Biometric Information Privacy Act, Section 5 e Section 15; v. City and County of San Francisco, Ordinance N. 103-19 (2019); cfr. D. LEVIN, *Face the facts, or is the face a fact?: biometric privacy in publicly available data*, in Fordham Intellectual Property, Media and Entertainment Law Journal, vol. 32, n. 4, 2022, pag. 1032 ss. 1043 ss.; cfr. W. HARTZOG, *BIPA: the most important biometric privacy law in the US?*, in A. Kak (a cura di), *Regulating Biometrics: Global Approaches and Urgent Questions*, 2020, pag. 96 s.

facciale in relazione a manifestazioni, proteste o forme di mobilitazione politica può incidere indirettamente sulla libertà di espressione e di riunione, producendo un effetto dissuasivo non dissimile da quello già rilevato in altri ordinamenti. A ciò si aggiunge il problema dell'accuratezza algoritmica: il GAO ha richiamato le preoccupazioni emerse nella letteratura tecnica e nel dibattito pubblico circa la diversa affidabilità dei sistemi rispetto a gruppi demografici differenti, con il conseguente rischio di trattamenti diseguali o di errori suscettibili di incidere soprattutto su soggetti già esposti a pratiche discriminatorie²⁷⁴. Anche recenti interventi delle autorità federali di tutela dei consumatori, come il caso Rite Aid deciso dalla Federal Trade Commission, mostrano come l'uso commerciale del riconoscimento facciale possa produrre danni rilevanti in assenza di ragionevoli salvaguardie, verifiche di accuratezza e misure di prevenzione dei falsi positivi²⁷⁵.

Il caso americano, quindi, mostra un modello innovativo perché è strutturalmente diverso dagli altri considerati. Negli Stati Uniti il rischio giuridico non si manifesta nella forma di un monopolio pubblico centralizzato della sorveglianza, bensì nella combinazione tra innovazione privata, utilizzo pubblico della tecnologia e regolazione frammentata tra vari livelli di governo. Questa combinazione dimostra come l'assenza di una disciplina organica e l'affidamento dello sviluppo tecnologico al mercato non riducano i rischi per i diritti fondamentali, ma possano favorire la diffusione di pratiche biometriche difficilmente riconducibili entro limiti unitari e garanzie effettive²⁷⁶.

5. *Il modello russo e il caso Glukhin c. Russia della Corte EDU*

Nel panorama comparato, l'esperienza russa assume particolare rilievo in quanto mostra come il riconoscimento facciale possa essere progressivamente assorbito entro

²⁷⁴ Cfr. U.S. Government Accountability Office, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522, 2020, pag. 1 s., 42; cfr. C. GARVIE, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Georgetown Law Center on Privacy & Technology, 2019, pag. 13 s.

²⁷⁵ V. Federal Trade Commission, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards*, 19 dicembre 2023; cfr. U.S. Government Accountability Office, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522, 2020, pag. 1 s.

²⁷⁶ Cfr. U.S. Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, GAO-23-105607, 2023, pag. 1 s., 12 ss., 36 ss.; cfr. U.S. Government Accountability Office, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522, 2020, pag. 42; cfr. D. LEVIN, *Face the facts, or is the face a fact?: biometric privacy in publicly available data*, in Fordham Intellectual Property, Media and Entertainment Law Journal, vol. 32, n. 4, 2022, pag. 1063 s.

un più ampio apparato di sorveglianza pubblica, formalmente giustificato da esigenze di sicurezza ma suscettibile di incidere in modo penetrante sulla vita privata e sull'esercizio delle libertà civili e politiche²⁷⁷. In questo contesto, la città di Mosca rappresenta il laboratorio più significativo: la rete di videosorveglianza urbana della capitale è stata progressivamente integrata con algoritmi di identificazione biometrica ed è arrivata a costituire uno dei più estesi sistemi di controllo visivo dell'area europea²⁷⁸. In particolare, una parte di tale infrastruttura è stata descritta come operante mediante Sphere²⁷⁹, una tecnologia che converte l'immagine del volto in una sorta di chiave biometrica e la confronta con le banche dati delle autorità, trasmettendo eventuali corrispondenze alle forze di polizia²⁸⁰. In linea generale, molte ricostruzioni concordano nel rilevare che il sistema moscovita combina telecamere diffuse nello spazio urbano e nei trasporti pubblici con software di riconoscimento facciale in grado di estrarre, comparare e verificare le immagini rispetto agli archivi delle forze dell'ordine, rendendo possibile un monitoraggio capillare degli spazi pubblici²⁸¹.

L'elemento più significativo dal punto di vista comparato non risiede nella sola esistenza di una rete tecnologicamente avanzata, quanto nelle modalità concrete del suo impiego. Diverse ricostruzioni hanno evidenziato che l'impiego del riconoscimento facciale a Mosca non è rimasto confinato alla repressione di reati gravi o all'identificazione di soggetti già ricercati, ma è stato impiegato anche nella gestione del dissenso e del controllo politico dello spazio pubblico²⁸². Un'inchiesta giornalistica internazionale ha documentato l'uso di tali strumenti per individuare e fermare

²⁷⁷ Cfr. O. A. STEPANOV, D.A. BASANGOV, *Smart digital facial recognition systems in the context of individual rights and freedoms*, in *Legal issues of Digital Age*, vol. 6, n. 2, 2025, pag. 118 ss.

²⁷⁸ Cfr. *Biometrics as a Kremlin tool*, in *Riddle Russia* (www.ridl.it), 5 maggio 2023, pag. 3 ss.; cfr. O. A. STEPANOV, D.A. BASANGOV, *Smart digital facial recognition systems in the context of individual rights and freedoms*, in *Legal issues of Digital Age*, vol. 6, n. 2, 2025, pag. 121 s.

²⁷⁹ La denominazione "Sphere" è qui utilizzata in senso circoscritto, con riferimento alla tecnologia di riconoscimento facciale impiegata nel contesto della metropolitana di Mosca, e non come sinonimo dell'intero sistema urbano di videosorveglianza e identificazione biometrica sviluppato nella capitale russa.

²⁸⁰ V. *How the facial recognition systems is arranged in Moscow*, in TAdviser (www.tadviser.com), sezione 2024, voce *The facial recognition system for 3.5 years helped identify about 1.5 thousand criminals in Moscow*, febbraio 2024

²⁸¹ Cfr. O. A. STEPANOV, D.A. BASANGOV, *Smart digital facial recognition systems in the context of individual rights and freedoms*, in *Legal issues of Digital Age*, vol. 6, n. 2, 2025, pag. 121 ss.; cfr. *Biometrics as a Kremlin tool*, in *Riddle Russia* (www.ridl.it), 5 maggio 2023, pag. 3 ss.

²⁸² Cfr. L. MASRI, *How facial recognition is helping Putin curb dissent*, special report, Settembre 2022; cfr. *Biometrics as a Kremlin tool*, in *Riddle Russia* (www.ridl.it), 5 maggio 2023, pag. 4

oppositori e partecipanti a manifestazioni, anche in funzione preventiva a seguito dell'inizio della guerra contro l'Ucraina, e analogamente altre analisi hanno evidenziato come il sistema sia stato impiegato per rintracciare attivisti, manifestanti e soggetti sottrattisi alla mobilitazione. Dunque, il riconoscimento facciale non è impiegato come mero ausilio tecnico all'attività investigativa, ma come tecnologia inserita in un più ampio apparato pubblico di sorveglianza potenzialmente orientato anche al contenimento del dissenso²⁸³.

Da un punto di vista formale, tale sviluppo si innesta in un ordinamento che riconosce sul piano costituzionale alcune garanzie rilevanti in materia di vita privata. La Costituzione della Federazione Russa del 1993 tutela all'articolo 23 il diritto alla vita privata, alla segretezza della corrispondenza, delle comunicazioni telefoniche, postali, telegrafiche e di altro tipo, ma anche la protezione dell'onore e della reputazione, mentre all'articolo 24 viene stabilito che la raccolta, conservazione, uso e diffusione di informazioni sulla vita privata di una persona non possono avvenire senza il suo consenso. A tali disposizioni si affianca la Federal Law n. 152-FZ del 2006²⁸⁴ che costituisce la disciplina generale in materia di protezione dei dati personali, e regola tra l'altro anche i dati biometrici, prevedendo il consenso dell'interessato e l'adozione di misure di sicurezza, ma ammette deroghe significative in funzione della sicurezza statale, dell'ordine pubblico e altre finalità pubblicistiche: è proprio in questa tensione tra garanzie proclamate e ampie deroghe che si colloca una delle principali criticità del modello russo²⁸⁵.

La dottrina che più di recente si è occupata del tema ha osservato come il sistema giuridico russo non offra – ancora – una disciplina sufficientemente puntuale sull'identificazione biometrica remota nello spazio pubblico, ed è stato sottolineato

²⁸³ Cfr. L. MASRI, *How facial recognition is helping Putin curb dissent*, special report, Settembre 2022; cfr. Human Rights Watch, *Russia: broad facial recognition use undermines rights*, settembre 2021, in HRW (www.hrw.org); cfr. *Biometrics as a Kremlin tool*, in Riddle Russia (www.ridl.it), 5 maggio 2023, pag. 4 s.

²⁸⁴ V. Costituzione della Federazione russa, artt. 23 e 24; v. Federal Law n. 152-FZ on Personal Data, 27 luglio 2006, artt. 9, 10, 11; cfr. S. MEDVEDEV, S. RUMYANTSEV, *Data protection in the Russian Federation: overview*, in Thomson Reuters Practical Law (www.uk.practicallaw.thomsonreuters.com), pag. 1 s., 3 s., 10 ss.

²⁸⁵ Cfr. S. MEDVEDEV, S. RUMYANTSEV, *Data protection in the Russian Federation: overview*, in Thomson Reuters Practical Law (www.uk.practicallaw.thomsonreuters.com), pag. 1 s.; cfr. O. A. STEPANOV, D.A. BASANGOV, *Smart digital facial recognition systems in the context of individual rights and freedoms*, in Legal issues of Digital Age, vol. 6, n. 2, 2025, pag. 122 ss.

che lo sviluppo dei sistemi intelligenti è proceduto più rapidamente della loro regolazione giuridica, con la conseguenza che il trattamento automatizzato delle immagini facciali e dei dati biometrici si sviluppa in un quadro normativo frammentato e non sempre idoneo a delimitare in modo preciso poteri, finalità, modalità d'uso e garanzie²⁸⁶.

In questo contesto si colloca il caso *Glukhin c. Russia*, deciso dalla Corte europea dei diritti dell'uomo nel luglio 2023, in cui il ricorrente, Nikolay Sergeyevich Glukhin, fu identificato dalle autorità russe dopo aver preso parte a una manifestazione individuale nella metropolitana di Mosca con un cartonato recante un messaggio politico²⁸⁷. Secondo quanto ricostruito in giudizio, la polizia aveva utilizzato immagini provenienti da un canale Telegram e dalle telecamere della metropolitana al fine di identificarlo, e in un secondo momento aveva impiegato il riconoscimento facciale in tempo reale per localizzarlo e procedere al suo arresto²⁸⁸. La vicenda, quindi, rileva sia per il fatto concreto, sia perché mostra come l'identificazione biometrica venga usata per reprimere una forma di espressione politica pacifica²⁸⁹. La Corte ha ritenuto violati gli articoli 8 e 10 CEDU:

- Sotto il primo profilo, è stato attribuito peculiare rilievo all'impiego del riconoscimento facciale, rilevando che la normativa russa non imponeva limiti sufficientemente chiari circa l'uso di tali tecnologie, né prevedeva adeguate garanzie procedurali contro abusi. La normativa russa, quindi, risulta carente in merito al requisito della *quality of law*²⁹⁰.
- Sotto il secondo profilo, ha osservato che la manifestazione del ricorrente riguardava una questione di interesse pubblico e che l'intervento repressivo delle autorità russe non era necessario in una società democratica, anche perché

²⁸⁶ Cfr. O. A. STEPANOV, D.A. BASANGOV, *Smart digital facial recognition systems in the context of individual rights and freedoms*, in *Legal issues of Digital Age*, vol. 6, n. 2, 2025, pag. 123 ss.

²⁸⁷ V. *Glukhin v. Russia*, App. no. 11519/20, ECtHR, 4 luglio 2023, par. 7

²⁸⁸ V. Corte EDU, sez. III, sent. 4 luglio 2023, *Glukhin c. Russia*, ric. n. 11519/20, in *Hudoc* (www.hudoc.echr.coe.int), par. 71, 72

²⁸⁹ V. Corte EDU, sez. III, sent. 4 luglio 2023, *Glukhin c. Russia*, ric. n. 11519/20, in *Hudoc* (www.hudoc.echr.coe.int), par. 71, 71, 88, 89

²⁹⁰ V. Corte EDU, sez. III, sent. 4 luglio 2023, *Glukhin c. Russia*, ric. n. 11519/20, in *Hudoc* (www.hudoc.echr.coe.int), par. 39, 78, 82, 83, 86, 88, 89

il comportamento contestato non aveva prodotto alcuna alterazione della vita pubblica²⁹¹.

Il rilievo comparato del caso in esame emerge, quindi, in modo netto: mostra come l'integrazione del riconoscimento facciale nelle reti urbane di videosorveglianza non incide solo sulla sfera della privacy individuale, ma si può riflettere direttamente anche sulle libertà politiche e sulla partecipazione nello spazio pubblico²⁹². Il caso Glukhin c. Russia non rappresenta un episodio isolato, bensì il momento in cui un problema strutturale del modello russo diventa giuridicamente visibile sul piano europeo: l'uso dell'identificazione biometrica, in assenza di una base normativa sufficiente e di garanzie effettive, finisce per rafforzare un apparato di controllo pubblico incompatibile con gli standard richiesti in una società democratica²⁹³.

²⁹¹ V. Corte EDU, sez. III, sent. 4 luglio 2023, *Glukhin c. Russia*, ric. n. 11519/20, in Hudoc (www.hudoc.echr.coe.int), par. 51, 54, 55, 56

²⁹² V. Corte EDU, sez. III, sent. 4 luglio 2023, *Glukhin c. Russia*, ric. n. 11519/20, in Hudoc (www.hudoc.echr.coe.int), par. 56, 88, 89; cfr. M. ZALNIERIUTE, *Glukhin c. Russia. App. n. 11519/20. Judgment*, in American Journal of International Law, 2023, pag. 695 ss.

²⁹³ V. Corte EDU, sez. III, sent. 4 luglio 2023, *Glukhin c. Russia*, ric. n. 11519/20, in Hudoc (www.hudoc.echr.coe.int), par. 82, 83, 88, 89; cfr. O. A. STEPANOV, D.A. BASANGOV, *Smart digital facial recognition systems in the context of individual rights and freedoms*, in Legal issues of Digital Age, vol. 6, n. 2, 2025, pag. 122 ss.; cfr. M. ZALNIERIUTE, *Glukhin c. Russia. App. n. 11519/20. Judgment*, in American Journal of International Law, 2023, pag. 697 s.

Conclusioni

L'analisi svolta nel presente elaborato consente di affermare che i sistemi di riconoscimento facciale rappresentano oggi uno dei punti più sensibili del rapporto tra innovazione tecnologica e tutela della persona. Non si tratta, infatti, di una semplice evoluzione delle tradizionali tecniche di videosorveglianza, ma di una trasformazione qualitativa del fenomeno del controllo: il volto umano viene convertito in dato biometrico, cioè in un'informazione suscettibile di essere di raccolta, elaborata, confrontata e conservata tramite procedure automatizzate. Proprio il passaggio dall'immagine al dato rende il fenomeno giuridicamente peculiare e spiega perché il riconoscimento facciale sollevi problemi non riducibili a una pura questione tecnica.

Già la ricostruzione iniziale della tecnologia ha consentito di evidenziare che il riconoscimento facciale non è uno strumento neutro. La sua specificità non risiede soltanto nella capacità di osservare, ma soprattutto in quella di identificare. Il volto, da elemento visibile della persona, viene tradotto in un modello biometrico confrontabile con altri modelli presenti in una banca dati, rendendo così possibile un'identificazione automatica tanto in tempo reale quanto in forma differita. Ne deriva che la rilevanza giuridica della tecnologia non dipende solo dalla raccolta dell'immagine, ma dalla possibilità di trasformare la presenza fisica dell'individuo in informazione stabile, interrogabile e collegabile ad altri dati. Il riconoscimento facciale non deve però essere necessariamente respinto in quanto tale: questi sistemi possono svolgere funzioni utili in determinati contesti, come la verifica dell'identità, la protezione di infrastrutture sensibili, la semplificazione di alcuni servizi o il supporto ad attività investigative. Una posizione di radicale chiusura nei confronti della tecnologia non appare, dunque, pienamente convincente in quanto rischierebbe di trascurare le potenzialità positive che l'innovazione può offrire dal punto di vista dell'efficienza, della sicurezza e dell'organizzazione dei servizi. Il punto critico, tuttavia, è che l'utilità dello strumento non può mai essere valutata in astratto, ma deve essere verificata alla luce del contesto d'uso, delle finalità perseguite, dei soggetti che lo impiegano e dell'intensità dell'impatto sui diritti fondamentali.

L'apparente oggettività dei sistemi, peraltro, non va confusa con una loro reale neutralità. Il riconoscimento facciale è progettato, addestrato e usato da soggetti umani,

sulla base di dati, finalità e criteri selezionati a monte. Anche quando l'identificazione appare come il risultato di un calcolo, essa riflette scelte tecniche, organizzative e istituzionali che devono poter essere controllate. Per questo, tali tecnologie non possono essere rimesse alla sola fiducia nella loro efficienza, ma esigono regole che ne rendano verificabili le condizioni di funzionamento e contestabili gli esiti.

L'indagine sui diritti fondamentali coinvolti ha mostrato che il riconoscimento facciale incide su una pluralità di posizioni giuridiche. Esso riguarda anzitutto la riservatezza e la protezione dei dati personali, in quanto consente il trattamento di informazioni biometriche idonee a identificare univocamente la persona. Il problema, tuttavia, non si esaurisce nella sola dimensione informativa: la trasformazione del volto in modello biometrico coinvolge anche la dignità umana in quanto il corpo non può essere ridotto a semplice supporto tecnico dell'identificazione, inoltre quando la tecnologia viene impiegata nello spazio pubblico può incidere sulla libertà di circolazione, riunione, associazione e manifestazione di pensiero producendo forme di condizionamento indiretto e fenomeni di autocensura. A ciò si aggiungono i rischi legati al principio di eguaglianza e al divieto di discriminazione specie quando l'accuratezza dei sistemi varia in relazione alle caratteristiche demografiche degli individui o quando le banche dati usate per il confronto biometrico non risultano rappresentative della popolazione generale.

I quadri normativi europeo e nazionale offrono strumenti importanti per contenere tali rischi. Il GDPR assicura una protezione rafforzata dei dati biometrici e impone il rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, necessità e proporzionalità. L'AI Act, a sua volta, introduce una logica ulteriore, fondata sulla classificazione del rischio e sulla previsione di obblighi specifici per i sistemi di intelligenza artificiale ad alto rischio. Anche l'ordinamento italiano attraverso il Codice privacy, l'attività del Garante e le più recenti disposizioni in materia di intelligenza artificiale, contribuisce alla costruzione di una cornice di tutela. Tuttavia, proprio l'analisi svolta dimostra che il quadro non può ancora considerarsi pienamente soddisfacente, soprattutto rispetto agli impieghi più invasivi del riconoscimento facciale.

La principale criticità risiede nel fatto che la tecnologia evolve con rapidità, mentre il diritto tende spesso a intervenire in modo successivo, frammentario o mediante categorie generali. Per quanto i principi generali restino indispensabili, da soli rischiano di non essere sufficienti quando si tratta di strumenti capaci di incidere in modo così intenso sull'identità, sulla libertà e sull'eguaglianza delle persone. Una regolazione effettiva dovrebbe dunque tradurre tali principi in garanzie operative più precise, distinguendo tra autenticazione e identificazione, tra uso differito e uso in tempo reale, tra impiego pubblico e privato, tra finalità amministrative, commerciali, di sicurezza o investigative.

Proprio da questa esigenza di traduzione operativa dei principi discende una riflessione più ampia sulle tecniche di produzione e aggiornamento della disciplina. Dinanzi a tecnologie soggette a mutamenti costanti, il diritto non può limitarsi a intervenire quando le prassi applicative si sono già consolidate, né può affidarsi esclusivamente a principi generali destinati a essere applicati caso per caso. I principi restano indispensabili, perché garantiscono continuità assiologica al sistema e consentono di mantenere ferma la centralità della persona, tuttavia, devono essere accompagnati da regole operative capaci di adattarsi alla rapidità dell'innovazione. Sarebbe auspicabile un modello di regolazione articolato su più livelli. Alla fonte legislativa dovrebbe spettare il compito di fissare le scelte fondamentali: i limiti all'impiego del riconoscimento facciale, le finalità ammissibili, le ipotesi vietate, le garanzie minime, i presupposti di necessità e proporzionalità e i rimedi a disposizione dell'interessato. Accanto, potrebbero però trovare spazio strumenti di aggiornamento più agili, fondati su un lavoro di raccordo tra competenze giuridiche, tecniche e istituzionali, capaci di tradurre i principi in prescrizioni concrete e periodicamente verificabili. Ciò non significherebbe sottrarre la materia al controllo democratico, né affidarla a una regolazione meramente tecnica, al contrario, proprio la complessità del riconoscimento facciale rende necessario che il legislatore sia affiancato da competenze specialistiche in grado di valutare l'evoluzione dei sistemi, la qualità dei dati, i tassi di errore, le modalità di verifica umana, la sicurezza degli archivi e l'impatto effettivo sui diritti fondamentali. Una disciplina realmente efficace dovrebbe quindi combinare la stabilità delle garanzie legislative con una capacità di aggiornamento costante delle regole applicative. In mancanza di tale manutenzione normativa, il rischio è duplice: da un

lato, quello di lasciare eccessivo spazio a prassi amministrative o private non sufficientemente controllate; dall'altro, quello di affidare la tutela dei diritti quasi esclusivamente agli interventi successivi delle autorità di controllo o della giurisprudenza. Una regolazione tempestiva e specializzata consentirebbe invece di anticipare i rischi, evitando che la protezione della persona intervenga solo dopo che l'uso della tecnologia si sia già normalizzato.

L'analisi dei casi italiani conferma questa esigenza. Il caso SARI mostra come l'identificazione biometrica in ambito di pubblica sicurezza richieda una base normativa chiara e specifica, soprattutto quando il sistema opera in tempo reale nello spazio pubblico. Al tempo stesso, l'uso differito di SARI Enterprise dimostra che anche strumenti meno invasivi rispetto alla sorveglianza in tempo reale possono sollevare problemi rilevanti, specie quando il confronto biometrico avviene rispetto a banche dati non neutrali o alimentate da pregresse attività di identificazione amministrativa e di polizia. Il caso Clearview AI evidenzia, invece, i rischi derivanti dalla raccolta massiva e indiscriminata di immagini online da parte di soggetti privati, mentre le esperienze di faceboarding e di riconoscimento facciale nei rapporti tra privati mostrano che non ogni impiego della tecnologia è necessariamente illecito, purché sia sorretto da volontarietà effettiva, alternative non biometriche, garanzie tecniche adeguate e limiti rigorosi di finalità e conservazione.

Anche il confronto internazionale conferma che non esiste un unico modo di regolare il riconoscimento facciale. L'esperienza cinese mostra il rischio di un'integrazione tra tecnologia biometrica, sicurezza pubblica e controllo sociale; il sistema Aadhaar indiano, così come le esperienze di Giamaica e Kenya, evidenziano come le infrastrutture di identità digitale possano essere presentate come strumenti di inclusione e modernizzazione, ma al tempo stesso generare rischi di esclusione e dipendenza amministrativa. Il modello statunitense mette in luce una diversa criticità, legata alla frammentazione normativa, all'innovazione privata e all'intervento spesso successivo delle garanzie, come dimostrano i casi Clearview AI e Williams. Il caso russo, infine, attraverso la vicenda Glukhin, mostra come il riconoscimento facciale possa diventare uno strumento di controllo dello spazio pubblico e di compressione delle libertà politiche quando sia impiegato senza una base normativa adeguata e senza garanzie effettive.

Il dato comparato conferma, quindi, che il problema del riconoscimento facciale non può essere affrontato mediante una risposta uniforme e astratta. È necessario distinguere tra contesti, finalità, soggetti utilizzatori e intensità dell'impatto sui diritti. Una tecnologia impiegata per la verifica volontaria dell'identità in un contesto delimitato non pone gli stessi problemi di un sistema di identificazione biometrica in tempo reale nello spazio pubblico; allo stesso modo, un uso amministrativo o commerciale non può essere valutato con gli stessi criteri di un impiego investigativo o di pubblica sicurezza. La regolazione deve quindi essere sufficientemente flessibile da non bloccare ogni forma di innovazione, ma anche abbastanza precisa da impedire che l'elasticità dei principi generali si traduca in una sostanziale normalizzazione della sorveglianza biometrica. In questa prospettiva, la posizione che emerge dall'analisi non è di rifiuto aprioristico della tecnologia, ma di favore condizionato e rigorosamente regolato. Il riconoscimento facciale può essere ammesso solo quando sia realmente necessario, proporzionato, fondato su una base giuridica adeguata e accompagnato da garanzie effettive. Tra queste assumono particolare importanza la trasparenza del trattamento, la qualità e rappresentatività dei dati, la misurazione dei tassi di errore, il controllo umano effettivo, la tracciabilità delle operazioni, la possibilità di contestare l'esito dell'identificazione e il divieto di fondare decisioni sfavorevoli esclusivamente sull'output del sistema. Senza tali condizioni, il rischio è che l'efficienza tecnologica prevalga sulla tutela della persona, trasformando uno strumento potenzialmente utile in un meccanismo di controllo difficilmente compatibile con un ordinamento fondato sui diritti fondamentali.

In conclusione, il riconoscimento facciale costituisce oggi uno dei banchi di prova più significativi per la capacità del diritto contemporaneo di confrontarsi con l'innovazione senza sacrificare la tutela effettiva della persona. Il problema fondamentale non è se il diritto debba arrestare l'innovazione, ma a quali condizioni essa possa essere governata senza alterare il nucleo essenziale dei diritti fondamentali. Proprio per questo, la sfida non consiste nello scegliere tra tecnologia e diritti, ma nel costruire regole capaci di orientare la tecnologia verso finalità legittime, impedendo che la rapidità del progresso tecnico lasci indietro le garanzie costituzionali. È in questo senso che il riconoscimento facciale si rivela non come un tema settoriale o marginale, ma come una questione paradigmatica del diritto del presente: una

questione nella quale si misura, in modo particolarmente evidente, la capacità dell'ordinamento di governare il progresso tecnologico senza rinunciare alla libertà, alla dignità e alla centralità della persona.

Bibliografia e sitografia

- Aa. Vv., *Bertillon Cards*, in *nlm.org*
- Aa. Vv., *Biometrics as a Kremlin tool*, in *ridl.it*, 2023
- Aa. Vv., *China's algorithms of repression: reverse engineering a Xinjiang police mass surveillance app*, in *hrw.org*, 2019
- Aa. Vv., *Facial recognition technology: current capabilities, prospects and governance*, in *nationalacademies.org*, 2024
- Aa. Vv., *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, in *fra.europa.eu*
- Aa. Vv., *How the facial recognition system is arranged in Moscow*, in *tadviser.com*, 2024
- Aa. Vv., *Russia: broad facial recognition use undermines rights*, in *hrw.org*, 2021
- ACLU MICHIGAN, *Facial recognition*, 2024
- ACLU, *Williams v. city of Detroit*, 2024
- AVITABILE A., *Il responsabile della protezione dei dati*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019
- BAILO F., *Welfare digitale: opportunità e prospettive dal diritto costituzionale*, in TROIANI L. (a cura di), *Politiche di welfare e costituzionalismo europeo. Il rapporto Beveridge ottant'anni dopo*, 2023
- BARLOW J.P., *A declaration of the independence of Cyberspace*, in *eff.org*
- BASSINI M., POLLICINO O., *La Cassazione sul "consenso algoritmico". Ancora un tassello nella costruzione di uno statuto giuridico composito*, in *giustiziainsieme.it*, 2021
- BHANDARI V., LAHIRI K., *The surveillance State, privacy and criminal investigation in India: possible futures in a post-Puttaswamy world*, in *University of Oxford human rights hub journal*, vol. 3(2), 2020
- BLED SOE W.W., *Facial recognition project report*, in Panoramic Research Inc., 1964
- BORGIA G., *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuri sviluppi normativi sul fronte eurounitario*, in *lalegislazionepenale.eu*, 2021

- BRAVO F., *Le condizioni di liceità di trattamento dei dati personali*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019
- BUOLAMWINI J., GEBRU T., *Gender shades: intersectional accuracy disparities in commercial gender classification*, in *Proceedings of machine learnings research*, vol. 81, 2018
- BYGRAVE L.A., *EU data protection law*, USA, 2002
- CARPINETO P., *La tutela dell'ambiente nella Costituzione italiana*, 2016
- CATALETA A., *Categorie particolari di dati: le regole generali e i trattamenti specifici*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019
- CELESTE E., *Digital constitutionalism: a new systematic theorization*, in *International review of law, computers & technology*, 2019
- COLACURCI M., *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche tra poteri pubblici, imprese e cittadini*, in *sistemapenale.it*, fascicolo 9/2022
- COLUCCINI R., GIANNINI A., SOTTILE L., *Il Viminale ci tiene all'oscuro su come e quanto usa il sistema di riconoscimento facciale*, in *irpimedia.irpi.eu*, 2024
- CREEMERS R., *China's emerging data protection framework*, in *Journal of cybersecurity*, 2022
- DIXON P., *A failure to "do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health Technol.*, 2017
- DUNN H.S., *Risking identity: a case study of Jamaica's short-lived national ID system*, in *Journal of information, communication and ethics in society*, vol. 18 n. 3, 2020
- EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR, *Call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination*, 2021
- ESPOSITO M.S., *Il trattamento transfrontaliero e la cooperazione tra le autorità garanti*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019

- FEDERAL TRADE COMMISSION, *Rite aid banned from using AI facial recognition after FTC says retailer deployed technology without reasonable safeguards*, 2023
- FEDERICO C.D., POPOLI A.R., *Le definizioni*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019
- FINOCCHIARO G., *Diritto dell'intelligenza artificiale*, Bologna, 2025
- FINOCCHIARO G., *Diritto di internet*, Torino, 2023
- FINOCCHIARO G., *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019
- FONSI A., *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante privacy sul sistema SARI Real Time*, in *penaledp.it*, n. 2/2021
- FORMICI G., *Digital welfare state and fundamental rights; the judicial litigation on digital identification systems in Kenya and Jamaica*, in *federalismi.it*, n. 26/2022
- GARVIE C., *Garbage in, garbage out: face recognition on flawed data*, in *Georgetown law center on privacy & technology*, 2019
- GIUSTINA C.D., *Il diritto all'ambiente nella Costituzione italiana*, in *ambientediritto.it*, 2020
- GLISIN N., MILASINOVIC S.M., LECIC B.N., *Artificial intelligence as a population surveillance tool: the case of China*, 2025
- GREENLAF G., *Global data privacy laws 2023: 162 national laws and 20 bills*, in *UNSW law research paper*, n. 23-48, 2023
- GREITENS S.C., *Dealing with demand for China's global surveillance exports*, in *Global China*, 2020
- GROTHER P., NGAN M., HANAOKA K., *Face recognition vendor test (FRVT), part 3: demographic effects*, NIST interagency report 8289, 2019
- GUARDIGLI E., *Le autorità di controllo: dalla direttiva 95/46/CE al Regolamento 679/2016*, in FINOCCHIARO G. (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019
- HARTZOG W., *BIPA: the most important biometric privacy law in the US?*, in KAK A. (a cura di), *Regulation biometrics: global approaches and urgent questions*, 2020
- HARTZOG W., SELINGER H., RHEE J.H., *Normalizing facial recognition technology and the end of obscurity*, in *European review of digital administration & law*, 2025

- HILL K., *Wrongfully accused by an algorithm*, in *The New York times*, 24 giugno 2020
- HU W., TAN T., WANG L., MAYBANK S., *A survey on visual surveillance of object motion and behaviors*, in *IEEE transactions on systems, man and cybernetics*, vol. 34, n. 3, 2004
- JAIN A.K., ROSS A., *Introduction to biometrics*, in JAIN A.K., FLYNN P., ROSS A. (a cura di), *Handbook of biometrics*, USA, 2008
- JAIN A.K., ROSS A., PRABHAKAR S., *An introduction to biometric recognition*, in *IEEE transaction on circuits and system for video technology*, vol. 14, n. 1, 2004
- JAIN U., *Right to privacy and the Aadhaar Act: a critical study*, in *Bharati law review*, 2018
- KERR O.S., *Four models of fourth amendment protection*, in *Standford law review*, vol. 60 n. 2
- KHERA R., *Impact of Aadhaar on welfare programmes*, in *Economic&Political Weekly*, vol. 52 n. 50, 2017
- KIILU N., *Indirect discrimination: Huduma Namba (digital identification) and the plight of the Nubian community in Kenya*, in *Streathmore law review*, vol. 7, 2022
- LEE J.A., ZHOU P., *FRT regulation in China*, in *Cambridge university press*, 2025
- LEVIN D., *Face the facts, or is the face the facts?: biometric privacy in publicly available data*, in *Fordham intellectual property, media and entertainment law journal*, vol. 32 n. 4, 2022
- MANTELERO A., *Artificial intelligence, dati e diritti: spunti di riflessione per i regolatori*, in BERTOLI P., FERRARI F., RIPAMONTI G., TIBERI G. (a cura di), *Data protection tra Unione europea, Italia e Svizzera*, Torino, 2019
- MARSICO G.M., *Violazione della normativa in tema di privacy e riservatezza: profili ricostruttivi sul divieto di riconoscimento facciale dei dipendenti ai fini della verifica delle presenze sul posto di lavoro*, in *rivistalabor.it*, 2024
- MASCOLO A., *Riconoscimento facciale e sicurezza pubblica: il dispositivo SARI*, in MACCHIA M. (a cura di), *Il presente dell'amministrazione algoritmica. Una ricerca sul campo*, Torino, 2026
- MASRI L., *How facial recognition is helping Putin curb dissent*, special report, 2022
- MEDVEDEV S., RUMYANTSEV S., *Data protection in the Russian federation: overview*, in *Thomson reuters practical law*

MOBILIO G., *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021

NAITO T., *Redifining the smart city for sustainable development*, in KHARAS H., MCARTHUR J., OHNO I. (a cura di), *Breakthrough. The promise of frontier technologies for sustainable development*, 2022

NATIONAL ACADEMIES OF SCIENCES, ENGINEERING AND MEDICINE, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, Washington DC

NORRIS C., MCCAHL M., WOOD D., *Editorial. The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space*, in *Surveillance & Society*, 2004

ONG R., *Privacy and personal information protection in China's all-seeing state*, in *International journal of law and information technology*, vol. 31/2023

PADMANABHAN A., SINGH V., *The Aadhaar verdict and the surveillance challenge*, in *Indian journal of Law and Technology*, vol. 15, 2019

PAGNANELLI V., *Decisioni algoritmiche e tutela dei dati personali. Riflessioni intorno al ruolo del Garante*, in *osservatorio sulle fonti*, n. 2/2021

PHILIPS J., RAUSS P.J., DER S.Z., *FERET, recognition algorithm development and test results*, in *nist.org*, 1996

PHILIPS P.J., GROTH P., MICHEALS R.J., BLACKBURN D.M., TABASSI E., BONE M., *Face recognition vendor test 2002: evaluation report*, in *nist.org*, 2003

PIZZETTI F., *La protezione dei dati personali dalla direttiva al nuovo regolamento. Una sfida per le autorità di controllo e una difesa per la libertà dei moderni*, in *medialaws.eu*

POLLICINO O., MUTO G., *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, in *medialaws.eu*, 2025

POLLICINO O., *Tutela dei diritti fondamentali nell'era digitale e contesto valoriale: una indagine transatlantica*, in *medialaws.eu*, 2018

QUARANTA M., *I sistemi di rilevazione di accessi e presenze con l'uso di dati biometrici sul posto di lavoro*, in *Diritto, economia e tecnologie della privacy*, anno VI, n. 3, 2015

RAJI I.D., FRIED G., *About face: a survey of facial recognition evaluation*, in *arxiv.org*, 2021

Redazione Britannica, *Alphonse Bertillon*, in *Encyclopaedia Britannica*

- Redazione Britannica, *François Vidocq*, in *Encyclopaedia Britannica*
- REZENDE I.N., *Facial recognition in police hands: assessing the “Clearview case” from a European perspective*, in *New Journal of European Criminal Law*, vol. 11, n. 3, 2020
- RICHARDS N., *The dangers of surveillance*, in *Harvard Law Review*, vol. 126 n. 7, 2013
- RODOTA’ S., *Elaboratori elettronici e controllo sociale*, Napoli, 2018
- RODOTA’ S., *Il diritto di avere diritti*, Roma, 2012
- RODOTA’ S., *Tecnologie e diritti*, Bologna, 2021
- RODOTA’ S., *Una costituzione per internet?*, in *Il Mulino – Rivisteweb*, n. 3/2010
- ROWE E.A., *Regulation facial recognition technology in the private sector*, in *Standford technology law review*, vol. 24:1, 2020
- SAVVIDES M., HEO J., PARK S.W., *Face Recognition*, in JAIN A.K., FLYNN P., ROSS A. (a cura di), *Handbook of biometrics*, USA, 2008
- SHI-KUPFER K., OHLBERG M., *China’s digital rise, challenges for Europe*, in *Merics papers on China*, n. 7, 2019
- SINGH V., *The Aadhaar verdict and the surveillance challenge*, in *Indian journal of law and technology*, vol. 15, 2019
- STANZIONE P., *Indagine conoscitiva sull’intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano*, Camera dei deputati, X Commissione, 2024, doc. web n. 9982816
- STANZIONE P., *Memoria del Presidente del Garante per la protezione dei dati personali*, 7 febbraio 2024, doc. web n. 9982816
- STEPANOV O.A., BASANGOV D.A., *Smart digital facial recognition systems in the context of individual rights and freedoms*, in *Legal issues of digital age*, vol. 6 n. 2, 2025
- STRALI, *Il caso trasparenza*, in *strali.org*
- TORRE J.D., *Quale spazio per I tools di riconoscimento facciale nella giustizia penale?*, in PAOLO G.D., PRESSACCO L. (a cura di), *Intelligenza artificiale e processo penale*, Trento, 2022
- U.S. GOVERNMENT ACCOUNTABILITY OFFICE, *Facial recognition services: federal law enforcement agencies should take actions to implement training and policies for civil liberties*

UNIQUE IDENTIFICATION AUTHORITY OF INDIA, *Annual report 2024-2025*

UNITED NATION HUMAN RIGHTS, OFFICE OF THE HIGH COMMISSIONER, *OHCHR assessment of human rights concerns in the Xinjiang Uyghur autonomous region, people's Republic of China, 2022*

WAYMAN J.L., *Biometric verification/identification/authentication/recognition: the terminology*, in LI S.Z., JAIN A. (a cura di), *Encyclopedia of biometrics*, 2009

YADAV R., VARSHNEY R., *Recalibrating the right to privacy in the digital age: legal challenges and constitutional safeguards in the era of technological intrusion*, in *ShodhKosh: journal of visual and performing arts*, 2024

ZALNIERIUTE M., *Glukhin c. Russia. App. n. 11519/20, Judgment*, in *American Journal of international law*, 2023

Giurisprudenza

Corte di Giustizia dell'Unione Europea

Corte di Giustizia, Grande Sezione, 9 novembre 2010, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen

Corte di Giustizia, Grande sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, Digital Rights Irlando LTD c. Minister for Communications, Marine and Natural resources and others e Kärntner Landesregierung and others

Corte di Giustizia, Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, Tele2 Sverige AB c. Post-och telestyrelsen e Secretary of State for the Home Department c. Tom Watson and others

Corte di giustizia, Sesta sezione, 9 febbraio 2023, C-453/21, X-FAB Dresden GmbH & Co. KG c. FC

Corte Europea dei Diritti Umani

Corte Europea dei diritti umani, Grande Camera, 25 maggio 2021, Big Brother Watch and Others c. Regno Unito

Corte Europea dei diritti umani, sez. III, 4 luglio 2023, Glukhin c. Russia

Corte Europea dei diritti umani, Grande Camera, 5 settembre 2017, Barbulescu c. Romania, ric. n.16496/08

Corte Europea dei diritti umani, Grande Camera, 17 ottobre 2019, Lopez Ribalda and others c. Spagna, ric. nn. 1874/13 e 8567/13

Corte Europea dei diritti umani, sez. III, 4 luglio 2023, Glukhin c. Russia, ric n. 11519/20

Corti nazionali

Corte di Cassazione italiana, sez. I, 27 maggio 1975, n. 2129

Corte di Cassazione italiana, sez. III, 9 giugno 1998, n. 5658

Corte di Cassazione italiana, Sez. Un., 6 ottobre 1979, n. 5172

Supreme Court of India, 24 agosto 2017, Justice K.S. Puttaswamy (Retd.) and Anr. V. Union of India and Ors., Writ Petition (Civil) n. 494 of 2012

Supreme Court of Judicature of Jamaica, Full Court, 12 aprile 2019, Julian J. Robinson v. The attorney general of Jamaica, claim no. 2018HCV01788

Katz v. Supreme Court of the United States, 18 dicembre 1967

Supreme Court of the United States, 22 giugno 2018, Carpenter v. United States

Settlement agreement, Williams v. city of Detroit, United States District Court for the Eastern District of Michigan, southern division, case no. 2:21-cv-10827, 28 giugno 2024

Normativa

Carta dei diritti fondamentali dell'Unione europea

Convenzione europea dei diritti dell'uomo

Trattato sul funzionamento dell'Unione europea

Regolamento (UE) 2016/679

Regolamento (UE) 2018/1725

Regolamento (UE) 2024/1689

Direttiva 95/46/CE

Direttiva 2016/680/UE

Costituzione italiana

Legge 31 dicembre 1996, n. 675

Legge 23 settembre 2025, n. 132

Legge 3 dicembre 2021, n. 205

Decreto Legislativo 20 giugno 2003, n. 196

Decreto Legislativo 9 settembre 2026, n. 160

Atto di Governo n. 418

Costituzione della Repubblica Popolare Cinese

Cybersecurity Law of the PRC

Costituzione Indiana

Digital Personal Data Protection Act, n. 22/2023

Costituzione giamaicana

Charter of fundamental rights and freedoms Act (Constitutional Amendment), 2011

Costituzione kenyota

Costituzione americana

Illinois Biometric information privacy act

City and county of San Francisco, ord. n. 103-19

Costituzione della federazione russa

Federal law n. 152-FZ on personal data

Soft law e documenti istituzionali

Consiglio d'Europa, Guidelines on facial recognition, 2021

Consiglio d'Europa, Commissione dei Ministri, Raccomandazione CM/Rec(2014)6

European Data Protection Board, Guidelines 05/2022, version 2.0

European Data Protection Board, Guidelines 03/2019, version 2.0

European Data Protection Board - European Data Protection Supervisor, Joint opinion 05/2021

European Data Protection Board - European Data Protection Supervisor, Call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination, giugno 2021

European Data Protection Board, Opinion 11/2024

WP29, Guidelines on Data Protection Officers

Allegato A al Provvedimento generale prescrittivo in tema di biometria, n. 513, 12 novembre 2014

Garante italiano per la protezione dei dati personali, parere n. 127, 25 marzo 2021, doc. web 9575877

Garante italiano per la protezione dei dati personali, ordinanza-ingiunzione 10 febbraio 2022, doc. web 9751362

Garante italiano per la protezione dei dati personali, provvedimento 11 settembre 2025, doc. web 10167745

Garante italiano per la protezione dei dati personali, provvedimento n. 16, 15 gennaio 2015

Garante italiano per la protezione dei dati personali, provvedimenti da 105 a 109 del 2024

Garante italiano per la protezione dei dati personali, provvedimento n. 531, 14 luglio 2026

Senato della Repubblica, Resoconto sommario n. 93, 30 luglio 2026

Presidenza del Consiglio dei Ministri, Comunicato stampa del Consiglio dei Ministri n. 185, voce "intelligenza artificiale"

European Data Protection Board (EDPB), *Overview of national supervisory authorities enforcement actions regarding Clearview AI, 2022- 2023* e nello

specifico, Decision by the Austrian SA against Clearview AI. Infringements articles 5, 6, 9 27 GDPR, 2023; Facial recognition: Italian SA fines Clearview AI EUR 20 milion, 2022; Hellenic DPA fines Clearview AI 20 milion euros, 2020; The French SA fines Clearview AI EUR 20 milion, 2022