NICOLA TRIGGIANI

Dubbi e perplessità sull'utilizzo investigativo e probatorio dei sistemi automatici di riconoscimento facciale nel procedimento penale dopo l'*AI Act* e la L. n. 132/2025*

Il saggio analizza le problematiche inerenti l'impiego dei sistemi automatici di riconoscimento facciale nel procedimento penale alla luce della disciplina introdotta dall'*AI Act* e dalla L. n. 132/2025, evidenziando le straordinarie potenzialità investigative di questi strumenti, ma al contempo le insidie e il rischio di abusi e lesioni dei diritti fondamentali della persona.

The Investigative and Evidentiary Use of Automated Facial Recognition Systems in Criminal Proceedings after the AI Act and Law No. 132/2025: Doubts and Concerns.

The paper examines the issues related to the use of automated facial recognition systems in criminal proceedings in light of the regulations introduced by the AI Act and Law No. 132/2025. It highlights the extraordinary investigative potential of these tools, while at the same time drawing attention to the pitfalls and risks of abuses and violations of fundamental human rights.

SOMMARIO: 1. Premessa definitoria. – 2. Il Sistema "S.A.R.I." (Sistema Automatico Riconoscimento Immagini) e gli interventi del Garante per la protezione dei dati personali. – 3. L'approvazione dell'*AI Act* (Regolamento europeo 1689/2024/UE) e gli usi consentiti e vietati dei sistemi automatici di riconoscimento facciale. – 4. La L. 23 settembre 2025, n. 132 e i tentativi di inquadramento giuridico del riconoscimento facciale automatizzato, tra tipicità e atipicità, nelle indagini preliminari e nel dibattimento, in attesa di una compiuta regolamentazione.

1. *Premessa definitoria*. Uno degli ambiti nei quali gli strumenti di intelligenza artificiale si stanno maggiormente affermando nel contesto del procedimento penale è, senza dubbio, la *digital evidence*: in particolare, nel più ampio quadro dei sistemi di identificazione biometrica[1], emergono i sistemi automatici di riconoscimento facciale, che possono essere definiti come dei *software* che, attraverso processi informatici basati sull'impiego di algoritmi, consentono di

*Questo lavoro è stato parzialmente sostenuto dal progetto FAIR - Future AI Research (PE00000013), nell'ambito del programma MUR del PNRR finanziato dal NextGenerationEU. Il contributo è destinato al volume collettaneo *Giustizia penale e intelligenza artificiale. Una riflessione sistemica*, a cura di Incampo-Triggiani, Bari, in corso di pubblicazione.

[1] I sistemi di identificazione biometrica, «attraverso l'analisi automatizzata delle caratteristiche fisiche (impronte digitali, volto, retina, iride), fisiologiche (ricavabili osservando le diverse funzioni corporee, cerebrali, battito cardiaco, respirazione) o comportamentali (ad es. scrittura, voce, cadenza dell'andatura), opportunamente convertite in dati digitali, permettono di comparare questi elementi distintivi al fine di identificare le persone»: così BELVINI, *Intelligenza artificiale e circuito investigativo*, Bari, 2025, 160. In argomento, v. anche, *ex plurimis*, SACCHETTO, *La prova biometrica*, in *La prova scientifica*, a cura di Conti-Marandola, Milano, 2023, 243 ss. e la bibliografia ivi citata.

stabilire – entro un certo margine di errore – la corrispondenza tra due immagini ritraenti il volto di una persona, consentendo così di identificare o verificare l'identità di un individuo in base alle sue caratteristiche fisionomiche[2].

[2] Così GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, in *Cass. Pen.*, 2025, 638 s.
La letteratura sul tema è ormai particolarmente ampia. Limitatamente a quella italiana, senza pretesa di completezza, cfr. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Leg. pen.*, 2021, 4, 206 ss.; COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sist. Pen.*, 2022, 9, 23 ss.; CURRAO, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Dir. pen. uomo*, 2021, 5, 68 ss.; DELLA TORRE, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?,* in *Intelligenza artificiale e processo penale: indagini, prove, giudizio*, a cura di Di Paolo-Presacco, Università degli Studi di Trento, Trento, 2022, 7 ss.; ID., *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, 41 ss.; DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, Milano, 2025; DI MATTEO, *La riservatezza dei dati biometrici nello spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, in *Freedom, Security & Justice: European Legal Studies*, 2023, 1, 74 ss.; ERRICO, *L'identificazione della persona nei cui confronti vengono svolte le indagini attraverso l'intelligenza artificiale (IA)*, in *Il processo*, 2025, 1, 371 ss.; LOPEZ, *La rappresentazione facciale tramite* software, in *Le indagini atipiche*[2], a cura di Scalfati, Torino, 2019, 239 ss.; MANGIARACINA, *Il riconoscimento facciale: nuove sfide nel processo penale*, in *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto, Atti del Convegno (Palermo, 18-19 aprile 2023)*, a cura di Di Simone-Mangiaracina-Parlato, Palermo, 2024, 77 ss.; MARANDOLA, *Il riconoscimento facciale*, in *La prova scientifica*, a cura di Marandola-Conti, cit., 500 ss.; MOBILIO, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?,* in *La democrazia nella società digitale. Tensioni e opportunità. Atti del Convegno 3 dicembre 2021*, a cura di Di Carpegna Brivio-Sancino, Torino, 2023, 1 ss.; ID., *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; PADOVA, *Il riconoscimento automatico del volto tra esigenze investigative e tutela della* privacy, in *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, a cura di Di Simone-Mangiaracina-Parlato, cit., 121 ss.; PALLANTE, *Le nuove sfide della cooperazione investigativa nello spazio europeo*, in *Sfide attuali e tendenze future del diritto processuale penale europeo*, a cura di Bernardini-De Caro, Torino, 2025, 257 ss.; PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *Media Laws*, 2021, 1, 204 ss.; PARLATO, *Il riconoscimento facciale: vantaggi e insidie alla luce della giurisprudenza della Corte EDU*, in *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, a cura di Di Simone-Mangiaracina-Parlato, cit., 95 ss.; SACCHETTO, Face to face*: il complesso rapporto tra automated facial recognition technology e processo penale*, in *www.lalegislazionepenale.eu*, 16 ottobre 2020, 1 ss.; EAD., *La capacità dimostrativa di un* match *di riconoscimento facciale nel procedimento penale alla luce del Regolamento (UE)2024/1689*, in *Sfide attuali e tendenze future del diritto processuale penale europeo*, a cura di Bernardini-De Caro, cit., 311 ss.; EAD., *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, Torino, 2025; SAPONARO, *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Arch. pen. web*, 2022, 1, 1 ss.; TESSITORE, *Riconoscimento automatico del volto e confronto in ambito forense*, in *120 Anni di polizia scientifica: l'identificazione personale tra scienza e diritto*, a cura di Di Simone-Mangiaracina-Parlato, cit., 61 ss.; TORRE, *Intelligenza artificiale e indagini penali: prospettive future e garanzie di sistema. Il sistema automatico di riconoscimento immagini*, in *Cybercrime*, a cura di Cadoppi-Canestrari-Manna-Papa, Milano, 2023, 1731 ss.; ID., *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 2021, spec. 1047 ss.; VALLI, *Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini*, in *www.IlPenalista.it*, 16 gennaio 2019; VASTA, *Diritto*

I *facial recognition system* operano, più precisamente, mediante algoritmi capaci di rilevare le c.d. *faceprint*, le impronte facciali, ovvero un certo numero di caratteristiche principali di un volto, quali la posizione di occhi, naso, narici, zigomi, mento, orecchie, e, in questa maniera, sono in grado di realizzare un "modello biometrico", cioè un modello digitalizzato del volto finalizzato al riconoscimento[3], una sorta di "codice a barre" dell'individuo, che può essere utilizzato con finalità identificative nelle attività sia di prevenzione che di accertamento dei reati, offrendo uno straordinario contributo all'attività investigativa. E, a differenza delle altre metodiche di identificazione biometrica basate sulle caratteristiche fisiologiche di un individuo, hanno un vantaggio evidente ovvero quello di non essere, almeno all'apparenza, strumenti invasivi, non determinando alcuna forma di coazione fisica diretta sulle persone, in quanto si può prescindere dalla collaborazione del destinatario[4].

Il riconoscimento automatico può avvenire attraverso due differenti modalità di funzionamento: la prima è la modalità statica (o *post remote* ovvero ricerca *off-line*, "a posteriori"), basata su immagini o video che sono già agli atti. Per la precisione, una foto di un soggetto con identità ignota viene ricercata all'interno di una banca dati precostituita contenente foto di soggetti con identità nota con l'obiettivo di trovare una corrispondenza tra la prima e una delle foto contenute nella banca dati, pervenendo così all'identificazione della persona ignota (confronto uno-a-molti)[5]: i dati vengono dunque trattati "in differita", successivamente alla raccolta.

La seconda è la modalità dinamica (o *real time*), fondata su immagini acquisite dal vivo e processate in tempo reale. Più esattamente, la lista di foto di soggetti da vagliare è confrontata istantaneamente e in maniera continua con tutti i volti individuati in uno o più flussi video provenienti da altrettante telecamere: nel caso in cui uno dei volti del video raggiunga un punteggio di somiglianza rispetto a quelli presenti nella "*watch list*" superiore ad una certa soglia (*match* di similarità), il sistema genera un *alert*.

Sul piano strettamente tecnico, prodromica alla vera e propria identificazione del soggetto interessato è la fase di analisi facciale, che si articola in diversi *step*: 1) acquisizione dell'immagine, che può avvenire con modalità diversifi-

---

dell'Unione europea e intelligenza artificiale. Riflessi sul procedimento penale, in *Riv. it. dir. proc. pen.*, 2024, 271 ss.

[3] Cfr., sul punto, tra gli altri, LOPEZ, *La rappresentazione facciale tramite* software, cit., 241.
Nel senso che il volto umano «costituisce il carattere più rappresentativo e individualizzante di un soggetto», ALESCI, *Il corpo umano fonte di prova*, Milano, 2017, 89.

[4] In tal senso v. MANGIARACINA, *Il riconoscimento facciale: nuove sfide nel processo penale*, cit., 78.

[5] In questi termini TESSITORE, *Riconoscimento automatico del volto e confronto in ambito forense*, cit., 62.

cate (volontariamente e in ambiente controllato oppure in maniera clandestina, all'insaputa del soggetto monitorato); 2) individuazione del volto all'interno dell'immagine (c.d. "*face detection*"), operazione che può rivelarsi particolarmente complessa nel caso in cui bisogna isolare l'immagine facciale da un *frame* di un video; 3) normalizzazione dell'immagine, che si sostanzia nel processo diretto ad attenuare le variazioni all'interno delle regioni del volto a causa dell'illuminazione o della posizione; 4) estrazione delle caratteristiche (c.d. "*features*") mediante le quali formare il modello (*template*) biometrico di riferimento; 5) registrazione dell'immagine e del modello biometrico all'interno del *database*; 6) confronto per misurare le somiglianze tra i diversi *template* biometrici registrati nel sistema[6].

2. *Il Sistema "S.A.R.I." (Sistema Automatico Riconoscimento Immagini) e gli interventi del Garante per la protezione dei dati personali.* Negli Stati Uniti già alla fine degli anni '90 e nei primi anni 2000 si discuteva dell'utilizzo dei dispositivi tecnologici di riconoscimento facciale automatizzato nell'ambito del processo penale; tuttavia il dibattito è divenuto particolarmente acceso nel 2020, quando è scoppiato lo "scandalo *Clearwiew*", dal nome della società statunitense che aveva creato un'*app* di riconoscimento facciale, utilizzata dalla polizia americana e dalle forze dell'ordine di diversi paesi europei, che operava su un *database* contenente miliardi di dati (foto, video, ecc.) "rubati" da *social network* come *Facebook*, *Twitter* e *Instagram* e altri siti web come *You Tube*. In sostanza, il *software* si basava su dati raccolti e trattati illegittimamente.

In Italia, su iniziativa del Ministero dell'interno-Dipartimento di pubblica sicurezza, dal 2016 è stato sviluppato il c.d. "sistema S.A.R.I." (acronimo di "Sistema Automatico Riconoscimento Immagini"), messo a disposizione delle forze di polizia, sulle cui specifiche tecniche di funzionamento, nonostante il suo impiego sia largamente diffuso sul territorio nazionale, viene mantenuto un sostanziale riserbo per non comprometterne l'efficacia e la sicurezza[7].

---

[6] Sul punto v., tra gli altri, DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 103 ss.; MARANDOLA, *Il riconoscimento facciale*, cit., 500 s.; MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 32 s.

[7] Come ricorda DIDDI, *E-Evidence, Data Base, Digital Investigation e AI*, Pisa, 2025, 164, nel 2018 l'Italia è venuta a conoscenza dell'esistenza di questi sistemi a seguito dell'arresto a Brescia di due soggetti ritenuti responsabili di un furto in appartamento, in quanto nel comunicato stampa si annunciava che ciò era stato possibile grazie al Sistema Automatico di Riconoscimento Immagini (S.A.R.I.) che «consente di effettuare ricerche nella banca dati A.F.I.S. (*Automated Fingerprint Identification System*) attraverso l'inserimento di un'immagine fotografica di un soggetto ignoto che, elaborata da due algoritmi di riconoscimento facciale, fornisce un elenco di immagini ordinato secondo un grado di similarità».

Esistono due modalità operative, distinte e separate, in cui si articola il *tool* in questione: il c.d. "S.A.R.I. *Enterprise*", che opera per la ricerca di volti a partire da immagini statiche su banche dati di grandi dimensioni; e il c.d. "S.A.R.I. *Real Time*", finalizzato al riconoscimento in tempo reale di volti presenti in flussi video provenienti da telecamere.

Più precisamente, con il sistema S.A.R.I. *Enterprise* le autorità sono messe in grado di ricercare entro 15 secondi l'identità di un volto, presente in un'immagine già acquisita agli atti, all'interno di una grandissima banca dati, individuata nella piattaforma A.F.I.S.-S.S.A., ovvero il sistema automatizzato di identificazione delle impronte digitali (*Automated Fingerprint Identification System*), integrato dal sotto sistema anagrafico, che contiene circa 20 milioni di cartellini fotosegnaletici (recanti una foto frontale e una foto del profilo destro). Al termine dell'operazione di raffronto, il sistema elabora un punteggio sul grado di similarità su una scala percentuale (*score*), restituendo un elenco di profili di candidati (c.d. "*candidate list*", in genere 50 profili) ordinati in base al livello di somiglianza con il soggetto da identificare.

Dunque, il sistema – come del resto tutti i sistemi di riconoscimento facciale automatizzato – offre «un 'ventaglio' di possibili corrispondenze espresso in termini probabilistici su base percentuale»[8]. E il riconoscimento è sempre sot-

---

Qualche informazione in più sull'applicativo si è potuta trarre indirettamente dal capitolato tecnico della procedura volta alla fornitura della soluzione integrata per il S.A.R.I., aggiudicata in favore di una società italiana nel 2017 (v. Ministero dell'Interno, *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il Sistema Automatico di Riconoscimento Immagini (S.A.R.I.)*, in *www.poliziadistato.it/statics/06/20160627-ct-sari-4-pdf*).

All'indomani della diffusione della notizia relativa allo scandalo *Clearwiew*, il 21 gennaio 2021, è stata rivolta una interrogazione parlamentare al Governo per conoscere se un *software* simile fosse in uso alle forze di polizia italiane: la risposta è stata negativa, precisando che era in uso esclusivamente il sistema S.A.R.I. *Enterprise* e che all'epoca nella banca dati A.F.I.S. erano presenti 17.592.769 cartellini fotosegnaletici, corrispondenti a 9.882.490 individui diversi. Nella risposta all'interrogazione il Ministro dell'Interno *pro tempore* ha spiegato il funzionamento del S.A.R.I. *Enterprise* e del S.A.R.I. *Real Time*, precisando però che quest'ultimo non è mai stato utilizzato, anche perché si attendeva una valutazione del Garante per la protezione dei dati personali (che ha dato poi parere negativo: v. *infra* nel testo). Il testo dell'interrogazione e la risposta del Ministro possono leggersi in *Atti parlamentari*, *XVIII legislatura* – resoconto stenografico dell'Assemblea – seduta n. 463 del 3 marzo 2021.

Ad ogni modo, come segnala BELVINI, *Intelligenza artificiale e circuito investigativo*, cit., p. 168, restano «ignote le modalità con le quali sono alimentate le banche date utilizzate per il raffronto automatizzato; non è affatto chiaro il destino delle immagini catturate dalla macchina ma di cui l'operatore ha escluso il *match* nel caso concreto, palesando così l'insidia di raccolte indiscriminate dei dati biometrici da utilizzare per ulteriori riconoscimenti; non sono note le metodologie con le quali è testata l'accuratezza del *software*; si concretizza, con il S.A.R.I. *Real Time*, il pericolo di monitoraggi clandestini su ampie fette della popolazione; non è dato sapere se vi sono accorgimenti per limitare gli accessi al *tool* né, tanto meno, se essi sono annotati in un apposito registro».

[8] DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 228.

toposto alla successiva verifica di un operatore-persona fisica esperto, tenuto a validare il risultato restituito dalla macchina, accertando che l'indice di similarità non rientri tra le anomalie statistiche, che la comparazione non abbia generato corrispondenze errate e che non siano subentrate interruzioni della "catena di custodia" o altre forme di alterazione del dato: ciò alla luce del divieto di decisioni totalmente automatizzate di cui agli artt. 11 Direttiva 680/2016/UE e 8 d.lgs. 18 maggio 2018, n. 51[9]. Dunque, l'eventuale corrispondenza riscontrata dal sistema con uno o più soggetti con caratteristiche facciali assimilabili a quelle del volto ignoto non ha alcuna conseguenza automatica, ma viene utilizzata per il prosieguo dell'attività investigativa.

Con il sistema S.A.R.I. *Real Time*, invece, è possibile acquisire in diretta le immagini dei volti inquadrati da telecamere (fisse o mobili) collocate in luoghi specifici oggetto di osservazione e confrontarli con un *database* più ristretto di persone ricercate (la c.d. "*watch list*", cioè una lista predefinita di persone "attenzionate", compilata di volta in volta in relazione all'evento da monitorare), la cui grandezza è al massimo di 10.000 volti. Il sistema può, più in particolare, essere installato direttamente nel luogo in cui sorga l'esigenza di disporre di una tecnologia di riconoscimento facciale per coadiuvare le forze di polizia nella gestione dell'ordine e della sicurezza pubblica o in relazione a specifiche esigenze investigative.

Allorquando la macchina riscontri una possibile corrispondenza positiva (*match*), viene a generarsi un segnale di allarme (*alert*), in grado di richiamare l'attenzione degli operatori, ai quali spetta il compito di confermare il riconoscimento e di prendere i provvedimenti conseguenti.

Va dunque evidenziato che, in entrambe le modalità, il riconoscimento deve essere sempre sottoposto alla successiva verifica di un operatore-persona fisica.

Ora, il S.A.R.I. *Enterprise* ha ottenuto nel 2018 il parere positivo del Garante per la protezione dei dati personali relativamente alla sua compatibilità con la disciplina in materia, sul rilievo che tale sistema non costituisce un nuovo trattamento di dati personali, in quanto si limita ad automatizzare alcune operazioni che prima richiedevano l'inserimento manuale di connotati identificati-

[9] Cfr. sul punto, tra gli altri, DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1078; DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 216 e 231 s., il quale sottolinea che si tratta di sistemi non «autosufficienti».

vi, consentendo le operazioni di ricerca nella banca dati A.F.I.S. attraverso il semplice inserimento di una fotografia[10].

È stata, invece, negativa la valutazione espressa dal Garante nel 2021 rispetto alla variante operativa *Real Time* del medesimo sistema, escludendone la conformità al d.lgs. 51/2018, attuativo della Direttiva 680/2016 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali da parte delle autorità competenti[11].

Al di là del riserbo sulle specifiche tecniche legate alle modalità di funzionamento – sulle quali si tornerà più avanti –, il Garante ha ritenuto di estrema delicatezza l'utilizzo di tecnologie di riconoscimento facciale per finalità di prevenzione e repressione dei reati nella modalità dinamica: «S.A.R.I. *Real Time* realizzerebbe un trattamento automatizzato su larga scala, che può riguardare anche persone presenti a manifestazioni politiche e sociali, che non sono oggetto di 'attenzione' da parte delle forze di polizia». Ed anche se nella valutazione di impatto, presentata al Garante dal Ministero degli interni, «si spiega che le immagini verrebbero immediatamente cancellate», nel provvedimento si ribadisce che «l'identificazione di una persona sarebbe realizzata attraverso il trattamento dei dati biometrici di tutti coloro che sono presenti nello spazio monitorato, allo scopo di generare modelli confrontabili con quelli dei soggetti inclusi nella '*watch-list*'. Si determinerebbe, così, una evoluzione della natura stessa dell'attività di sorveglianza, che segnerebbe un passaggio dalla sorveglianza mirata di alcuni individui alla possibile sorveglianza universale»[12].

SARI *Real Time* sarebbe suscettibile, pertanto, di violare i diritti fondamentali delle persone coinvolte. Il trattamento dei dati biometrici svolto da quest'ultimo applicativo è stato, dunque, definito illecito, essendo destituito di adeguata base normativa e non conforme alla normativa in materia di *data protection*.

---

[10] Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell'identità di un volto*, provvedimento del 26 luglio 2018, n. 440, doc. web 9040256.

[11] Garante per la protezione dei dati personali, *Parere sul sistema SARI Real Time*, provvedimento del 25 marzo 2021, n. 127, doc. web 9575877. A commento della decisione, v. FONSI, *Prevenzione dei reati e riconoscimento facciale: il parere sfavorevole del Garante* privacy *sul Sistema SARI* Real Time, in *Penale Dir e proc.*, 2021, 289 ss.; LOPEZ, *Videosorveglianza biometrica tramite riconoscimento facciale: parere negativo del Garante per la* privacy, in *Proc. pen. giust.*, 2022, 798 ss.; PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, cit., 213 ss.; RAFFIOTTA-BARONI, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in *BioLaw Journal – Riv. BioDir.*, 2022, 165 ss.

[12] Garante per la protezione dei dati personali, *Parere sul sistema SARI* Real Time, provvedimento del 25 marzo 2021, cit.

A seguito di questa seconda pronuncia del Garante, il legislatore ha introdotto una moratoria rispetto all'installazione e all'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso di dati biometrici, in luoghi pubblici o aperti al pubblico, sino all'entrata in vigore di una disciplina legislativa *ad hoc*, e comunque sino alla data del 31 dicembre 2023 (art. 9, co. 9 d.l. 8 ottobre 2021, n. 139, conv. con modif. 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*»), termine poi prorogato al 31 dicembre 2025 (art. 8-*ter* d.l. 10 maggio 2023, n. 51, conv. con modif. dalla L. 3 luglio 2023, n. 87, recante «*Disposizioni urgenti in materia di amministrazione di enti pubblici, di termini legislativi e di iniziative di solidarietà sociali*»), con alcune consistenti deroghe previste dall'art. 9, co. 12 d.l. n. 139/2021 con riferimento alle attività «di prevenzione e repressione dei reati»[13].

3. *L'approvazione dell'AI Act (Regolamento europeo 1689/2024/UE) e gli usi consentiti e vietati dei sistemi automatici di riconoscimento facciale.* Nel frattempo, com'è noto, il 13 giugno 2024 è stato approvato, dopo un lungo *iter*, il Regolamento n. 1689/2024/UE del Parlamento europeo e del Consiglio sull'intelligenza artificiale, noto come *AI Act* (pubblicato sulla G.U. dell'Unione europea il successivo 12 luglio)[14], che, nel quadro di un'ampia e organica regolamentazione dei sistemi di intelligenza artificiale, la prima a livello mondiale, ha offerto innanzitutto una definizione di intelligenza artificiale – cosa niente affatto scontata – nella quale risultano pienamente ricompresi i sistemi di riconoscimento facciale automatizzato.
A seconda delle loro caratteristiche tecniche, tali sistemi ricadono, alternativamente, nell'ambito delle pratiche vietate, in quanto «a rischio inaccettabile», di cui all'art. 5 Reg. 1689/2024, potendo rappresentare una minaccia grave per i diritti fondamentali, ovvero nell'ambito dei sistemi «ad alto rischio», di

[13] Sul punto, v., tra gli altri, DI MATTEO, *La riservatezza dei dati biometrici nello spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, cit., 110.
[14] Per un quadro d'insieme sulle problematiche relative al procedimento penale disciplinate dall'*AI Act*, v. CANZIO, AI Act *e processo penale: sfide e opportunità*, in *Prova scientifica e processo penale*[3], a cura di Canzio-Luparia Donati, Milano, 2025, 999 ss.; PINELLI, AI Act*: gestione del rischio e tutela dei diritti*, in *Giur. it.*, 2025, 452 ss.; QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'*AI Act, in *www.dirittodidifesa.eu*, 16 gennaio 2025; SCALFATI, *IA e processo penale: prospettive d'impiego e livelli di rischio*, in *Proc. pen. giust.*, 2024, 1404 ss.; TERESI, *L'*AI Act *nell'ottica del processualpenalista: uno sguardo preliminare*, in *Penale Dir. e proc.*, 2024, 3, 361 ss.; TORRE, *Il regolamento europeo sull'intelligenza artificiale: i profili processuali*, in *Proc. pen. giust.*, 2024, 1543 ss.

cui agli artt. 6 ss. Reg. 1689/2024, e sono prescritti specifici adempimenti sia ai fornitori (*provider*) che agli utilizzatori (*deployer*) al fine di garantire la conformità di questi ultimi sistemi a quanto previsto dal Regolamento.

Va accolta, innanzitutto, con grande favore la scelta del legislatore europeo di vietare in radice, in modo assoluto, pratiche come quelle che hanno portato allo scandalo *Clearview*, trattandosi di un livello di rischio ritenuto inaccettabile, in ragione della potenziale violazione di diritti fondamentali: ai sensi dell'art. 5, par. 1 lett. e) Reg. 1689/2024, infatti, non è consentito, in alcun caso, l'impiego di sistemi di A.I. che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping*, cioè il rastrellamento non mirato di immagini facciali estrapolate da *internet* o da filmati di telecamere a circuito chiuso. Tale pratica – come si legge nel *Considerando n. 43* – «accresce il senso di sorveglianza di massa e può portare a gravi violazioni di diritti fondamentali, compreso il diritto alla vita privata».

Nell'ambito delle pratiche vietate, ai sensi dell'art. 5, par. 1 lett. h) Reg. 1689/2024, rientrano anche i sistemi di identificazione biometrica remota «in tempo reale» in «spazi accessibili al pubblico»[15] a fini di attività di contrasto, così dovendosi intendere gli applicativi che – sul modello di SARI *Real Time* – consentono l'identificazione automatizzata della persona, mediante la comparazione di dati biometrici, tra i quali immagini facciali, in termini pressoché istantanei, attraverso il confronto con i dati presenti in archivio.

Tale divieto, tuttavia, non è assoluto, essendo l'impiego dei sistemi di riconoscimento facciale automatizzato "*real time*" consentito, alla luce del principio di proporzione, in caso di assoluta necessità al fine di perseguire uno degli obiettivi specificamente indicati nel seguito della disposizione, vale a dire: la ricerca mirata di specifiche vittime di gravi reati (sottrazione, tratta o sfruttamento sessuale di esseri umani), nonché la ricerca di persone scomparse (ricerca che potrebbe anche non avere alcun aggancio con la sfera penalistica)[16]; la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale attuale o pre-

[15] Per «spazio accessibile al pubblico», il Reg. 1689/2024/UE (*Considerando n. 19*) intende «qualsiasi luogo fisico accessibile a un numero indeterminato di persone fisiche e a prescindere dal fatto che il luogo in questione sia di proprietà pubblica o privata, indipendentemente dall'attività per la quale il luogo può essere utilizzato, quali il commercio (ad esempio negozi, ristoranti, bar), i servizi (ad esempio banche, attività professionali, ospitalità), lo sport (ad esempio piscine, palestre, stadi), i trasporti (ad esempio stazioni di autobus, metropolitane e ferroviarie, aeroporti, mezzi di trasporto), l'intrattenimento (ad esempio cinema, teatri, sale da concerto e sale conferenze), il tempo libero o altro (ad esempio strade e piazze pubbliche, parchi, foreste, parchi giochi)».

[16] Come sottolinea QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, cit., 9.

vedibile di un attacco terroristico (qui l'istanza è prettamente securitaria e preventiva, ma verosimilmente legata, per via delle caratteristiche di specificità richieste, a investigazioni già in corso per altri fatti); la localizzazione o l'identificazione di una persona sospettata di aver commesso determinati reati, espressamente elencati nell'Allegato II al Regolamento, ai fini dello svolgimento di una indagine penale, o dell'esercizio dell'azione penale o dell'esecuzione di una sanzione penale per tali reati, punibili nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata superiore nel massimo a quattro anni.

L'Allegato II, per la precisione, individua sedici categorie di illeciti per le quali è possibile l'impiego dei sistemi di riconoscimento facciale ai fini della localizzazione e/o identificazione di persone sospettate: terrorismo; tratta di esseri umani; sfruttamento sessuale di minori e pornografia minorile; traffico illecito di stupefacenti o sostanze psicotrope; traffico illecito di armi, munizioni ed esplosivi; omicidio volontario; lesioni gravi; traffico illecito di organi e tessuti umani; traffico illecito di materie nucleari e radioattive; sequestro, detenzione illegale e presa di ostaggi; reati che rientrano nella competenza giurisdizionale della Corte penale internazionale; illecita cattura di aeromobile o nave; violenza sessuale; reato ambientale; rapina organizzata o a mano armata; sabotaggio; partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati sopra elencati[17].

Ora, è vero che l'utilizzo da parte delle forze dell'ordine dei sistemi di identificazione biometrica remota in tempo reale richiede comunque l'autorizzazione preventiva dell'autorità giudiziaria[18] o di un'autorità amministrativa indipendente dello Stato membro, fatta salva, in casi di urgenza, la possibilità di una convalida *ex post*, richiesta, senza ritardo, entro le ventiquattro ore successive all'uso del sistema, dovendosi, in mancanza, procedere immediatamente a interrompere l'utilizzo, nonché all'eliminazione e alla cancellazione dei dati, dei risultati e degli *output* (art. 5, par. 3 Reg. 1689/2024). Ed è anche vero che l'attività può essere autorizzata, su richiesta motivata,

[17] DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 82, sottolinea che si tratta ovviamente di «indicazioni di carattere generale, che devono essere poi adeguate in base alla legislazione penalistica dei singoli Paesi, al fine di ricercare le fattispecie incriminatrici corrispondenti».

[18] In considerazione dei delicati interessi coinvolti, appare corretto ritenere che nel nostro sistema processuale l'autorizzazione debba provenire dal giudice procedente e, nella fase delle indagini preliminari, dal giudice per le indagini preliminari: in tal senso v. CANZIO, *AI Act e processo penale: sfide e opportunità*, cit., 1010; DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 84; TORRE, *Il regolamento europeo sull'intelligenza artificiale: i profili processuali*, cit., 1543.

dall'autorità giudiziaria o amministrativa competente, la cui decisione è vincolante, solo all'esito di un positivo vaglio di necessità e proporzionalità dell'uso del sistema di identificazione biometrica per il conseguimento di uno degli obiettivi per cui è consentita dal Regolamento e solo se l'autorità di contrasto abbia eseguito una valutazione di impatto sui diritti fondamentali e registrato il sistema nella relativa banca dati UE (art. 5, par. 2 Reg. 1689/2024).

Tuttavia, al di là dello sforzo del legislatore europeo per cercare di circoscrivere le eccezioni al divieto, appare evidente che le deroghe previste sono talmente generiche che rischiano, di fatto, di svuotare completamente di significato il divieto (non a caso, durante la discussione del testo, il Parlamento europeo aveva espresso assoluta contrarietà alla previsione di queste deroghe)[19].

In definitiva, «pare ragionevole immaginare che solo un estremo rigore interpretativo possa evitare un generalizzato ricorso al riconoscimento facciale in *real time*, in tutti i luoghi aperti al pubblico, con sostanziale rovesciamento del divieto pur scolpito nell'art. 5 par. 1 lett. h)» del Regolamento europeo sull'intelligenza artificiale[20].

All'art. 26, par. 10 Reg. 1689/2024 trova posto, invece, la disciplina dei sistemi di riconoscimento facciale che operano "a posteriori". Tale attività, valutata come ad "alto rischio", è consentita, ma solo al fine di ricercare «una persona sospettata o condannata per aver commesso un reato», ed è subordinata ad un'autorizzazione, *ex ante* o senza indebito ritardo ed entro quarantotto

[19] La sottolineatura è di QUATTROCOLO, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, cit., 9, la quale osserva altresì (8 s.): «Del resto la gamma di eccezioni giustifica, in primo luogo, la dotazione, in ogni possibile luogo pubblico, di telecamere 'di sicurezza', peraltro già ampiamente diffusa. Inoltre, il perseguimento delle finalità indicate nelle eccezioni finirebbe per legittimare sempre la ripresa di ciò che accade nel luogo pubblico, al fine di poter individuare, di volta in volta, la vittima di grave delitto, l'accusato o condannato di uno dei reati dell'Allegato II, il soggetto pericoloso...».
Sul punto, v. anche GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, cit., 668, il quale osserva che le previsioni del Regolamento europeo sull'intelligenza artificiale prevedono sì un ampio novero di requisiti e di condizioni di legittimità dell'uso dei sistemi di riconoscimento facciale in tempo reale o a posteriori, «ma, al contempo, sono contraddistinte da un notevole tasso di genericità e corredate da numerose previsioni derogatorie», sicché «non paiono delineare una disciplina sufficientemente stringente e in grado di 'resistere' a possibili tentativi di aggiramento»; nonché VASTA, *Diritto dell'Unione europea e intelligenza artificiale. Riflessi sul procedimento penale*, cit., 284, la quale osserva che «la formulazione letterale delle eccezioni al divieto, talora generica», presta il fianco a «rischi di disomogeneità applicativa nei diversi Stati membri», rischio che si può sicuramente presentare «anche rispetto alla possibilità di utilizzare il sistema per la ricerca degli autori di determinati reati individuati con riferimento al limite massimo edittale della pena, che muta a seconda delle legislazioni nazionali». Nello stesso senso, del resto, già SACCHETTO, Automated faced based human recognition tecnologies *e procedimento penale alla luce dell'*AI Act*: alcuni spunti di riflessione*, in *La via europea per l'intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche – Cà Foscari Venezia, 25-26 novembre 2021*, a cura di Camardi, Milano, 2022, 371, con riferimento alla Proposta di regolamento.

[20] Così, ancora QUATTROCOLO*, Intelligenza artificiale e processo penale: le novità dell'AI Act*, cit., 9.

ore, da parte di un'autorità giudiziaria o amministrativa, la cui decisione è vincolante e soggetta a controllo giurisdizionale. L'uso deve essere «limitato a quanto strettamente necessario per l'indagine su uno specifico reato». L'autorizzazione, tuttavia, non è richiesta quando il sistema di riconoscimento facciale automatizzato è utilizzato per l'«identificazione iniziale di un potenziale sospettato sulla base di fatti oggettivi e verificabili direttamente connessi al reato».

In ogni caso, «occorre garantire che nessuna decisione che produca effetti giuridici negativi su una persona possa essere presa dalle autorità di contrasto unicamente sulla base dell'*output* di tali sistemi di identificazione biometrica a posteriori»[21].

Il Reg. 1689/2024 – che fa salve le previsioni del diritto europeo in materia di protezione dei dati personali – introduce inoltre un'organica disciplina relativa all'immissione in commercio e all'impiego dei sistemi di intelligenza artificiale, prevedendo delle disposizioni intertemporali per l'entrata in vigore di alcune disposizioni, così da incoraggiare i legislatori nazionali dei singoli Stati membri a valutare l'introduzione di disposizioni di maggior dettaglio, in coerenza con le peculiarità dei singoli sistemi giuridici[22]. In particolare, l'art. 113 Reg. 1689/2024 prevede che le disposizioni in esso contenute si applichino a decorrere dal 2 agosto 2026, fatti salvi i capi I e II la cui decorrenza è stata anticipata al 2 febbraio 2025 (e vi è ricompreso dunque l'art. 5), mentre le previsioni di cui all'art. 6, par. 1 si applicano a decorrere dal 2 agosto 2027.

4. *La L. 23 settembre 2025, n. 132 e i tentativi di inquadramento giuridico del riconoscimento facciale automatizzato, tra tipicità e atipicità, nelle indagini preliminari e nel dibattimento, in attesa di una compiuta regolamentazione*. Il 10 ottobre 2025 è entrata in vigore la L. 23 settembre 2025, n. 132, recante «*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*», finalizzata ad armonizzare la normativa nazionale alle disposizioni dell'*AI Act*, nonché a definire una strategia nazionale per un corretto sviluppo di detta tecnologia in Italia[23].

---

[21] Sul punto, v. già il *Considerando n. 35* Reg. 1689/2024/UE.

[22] Cfr. sul punto. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, cit., 667, per il quale è indubbio che «le articolate disposizioni intertemporali previste dal Regolamento, volte a differire la cogenza delle disposizioni più qualificanti" siano proprio "finalizzate a consentire agli Stati membri di dotarsi di una disciplina armonica alle previsioni europee e, specie con riferimento alle garanzie procedurali minime da esse appena abbozzate, coerente con le peculiarità dei singoli sistemi giuridici».

[23] Tra i primi commenti, per quanto concerne i profili attinenti al procedimento penale, v. *Intelligenza artificiale e indagini penali. Strumenti, garanzie, responsabilità e scenari dell'innovazione investigativa*

L'art. 24, co. 1 L. 132/2025, prevede che, entro un anno dall'entrata in vigore della legge, il Governo sia delegato ad emanare uno o più decreti legislativi per l'adeguamento della normativa nazionale al Reg. 1689/2024/UE, con la previsione di un'apposita disciplina per l'utilizzo di sistemi di intelligenza artificiale per l'attività di polizia (art. 24, co. 2 lett. h) L. 132/2025).
Il Governo, a norma dell'art. 24, co. 3 L. 132/2025, è altresì delegato ad adottare, entro lo stesso termine, uno o più decreti legislativi per adeguare e specificare la disciplina dei casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale, prevedendo, tra l'altro, che l'utilizzo dei sistemi di intelligenza artificiale nelle indagini preliminari sia regolato nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei princìpi di proporzionalità, non discriminazione e trasparenza (art. 24, co. 5 lett. e) L. 132/2025) e la necessità di modificare conseguentemente, a fini di coordinamento e razionalizzazione del sistema, la normativa sostanziale e processuale (art. 24, co. 5 lett. f) L. 132/2025).
Allo stato, dunque, manca una espressa e precisa disciplina legislativa nazionale dei sistemi di riconoscimento facciale automatizzato, ed è difficile prevedere quando tale normativa sarà effettivamente operativa, considerando i tempi per l'attuazione delle deleghe al Governo e la necessità, poi, di una indispensabile disciplina attuativa di secondo grado per tutti i dettagli tecnici.
Quanto ai pareri del Garante per la protezione dei dati personali prima ricordati, è appena il caso di rilevare che sono ovviamente limitati alla tutela della *privacy*, lasciando dunque irrisolti gli snodi maggiormente rilevanti in ordine all'impiego dei sistemi di riconoscimento facciale automatizzato nel procedimento penale, con riferimento in particolare alla stessa idoneità epistemologica dello strumento, alle ricadute sulle altre libertà fondamentali, ai casi in cui tali sistemi sono utilizzabili[24].
Vi è anche una carenza di specifiche indicazioni giurisprudenziali in materia: se in altri ambiti la giurisprudenza costituzionale e di legittimità ha svolto una fondamentale opera di supplenza all'inerzia del legislatore, fissando precisi "paletti" a tutela dei diritti fondamentali – è il caso, ad es., delle videoriprese

digitale. Aggiornato con la l. 23 settembre 2025, n. 132. Disposizioni e deleghe al Governo in materia di intelligenza artificiale, a cura di Parodi-Rizzo, Milano, 2025.
[24] In questi termini, BELVINI, *Intelligenza artificiale e circuito investigativo*, cit., 169.

investigative[25] – questo non è (o perlomeno non è ancora) avvenuto con riferimento alle tecnologie di riconoscimento del volto[26].

Nelle poche decisioni di merito disponibili, ci si limita per lo più a dare atto dell'uso investigativo del *software* con finalità identificative, omettendo però di affrontare il quesito preliminare sulle norme abilitanti l'impiego del programma di A.I.[27], mentre la giurisprudenza di legittimità, nelle rare occasioni in cui ha avuto modo di occuparsi del tema, ha trascurato l'argomento o lo ha reputato comunque non decisivo nel caso specifico[28].

Ora, in attesa di una dettagliata regolamentazione nazionale ancora di là da venire, dal momento che il S.A.R.I. è comunque una realtà già operativa, e a quanto risulta, ampiamente utilizzata dalle forze di polizia e dalla polizia giu-

---

[25] Sul punto, sia consentito rinviare a TRIGGIANI, *Le videoriprese investigative tra Corte costituzionale e Sezioni Unite: cronaca di una travagliata evoluzione giurisprudenziale (...in attesa del legislatore)*, in *Iurisdictio*, 2023, 40 ss.

[26] In altri ordinamenti, invece, da tempo la giurisprudenza ha individuato alcune coordinate circa l'impiego delle tecnologie di riconoscimento facciale: è il caso, ad es., del Regno Unito, sul quale v. DELLA TORRE, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice *(ma raccoglie le critiche del Garante* privacy *d'oltremanica)*, in *Dir. pen. cont.*, 2020, 231 ss.; PIN, *Non esiste la "pallottola d'argento": l'*Artificial Face Recognition *al vaglio giudiziario per la prima volta*, in *DPCE on line*, 2019, 4, 3075 ss.

[27] Lo evidenzia BELVINI, *Intelligenza artificiale e circuito investigativo*, cit., 170 e nn. 77 e 78. Cfr. App. Roma, sez. II, 2 ottobre 2023, n. 10003, in *OneLegale*; Trib. Nola, 11 gennaio 2024, n. 2055, *ivi*, la quale accenna all'uso del S.A.R.I., dando atto che, dopo aver visionato le immagini acquisite dagli impianti di videosorveglianza di un istituto bancario, la polizia giudiziaria aveva inserito il fotogramma estrapolato dal video nel citato sistema in uso alla polizia scientifica e quest'ultimo aveva individuato delle somiglianze con l'imputato; Trib. Napoli, sez. VI, 26 settembre 2022, n. 8679, *ivi*; Trib. Ascoli Piceno, 20 luglio 2022, n. 452, *ivi*; Trib. Genova, sez. I, 26 febbraio 2022, n. 600, in *Guida dir.*, 2022, 36, 84.

[28] Cfr., da ultimo, Cass., Sez. II, 20 marzo 2025, n. 18099, in *www.terzultimafermata.blog*, 27 agosto 2025, la quale ha ritenuto infondato il ricorso dell'imputato che riteneva «illogico attribuire valenza indiziaria a una compatibilità solo del 55,2% tra le immagini di uno dei soggetti che erano stati ripresi dalle telecamere di videosorveglianza e l'immagine del proprio cartellino foto-segnaletico» (poiché, così facendo, secondo il difensore «[s]i entra nel concetto di probabilismo confinante con il possibilismo così non consentendo che dell'esito accertativo se ne possa dedurre un elemento a carico dell'imputato»), sul rilievo che nel caso di specie, nell'economia della decisione della Corte d'appello impugnata, gli esiti del riconoscimento facciale con il sistema S.A.R.I. avevano assunto solo il ruolo di uno dei plurimi riscontri individualizzanti alle dichiarazioni accusatorie che erano state rese nei confronti dell'imputato dai due coimputati. In motivazione la Corte ha richiamato un suo precedente (Cass., Sez. IV, 13 luglio 2023, n. 39551, in *De Jure*), che non ha escluso l'utilizzabilità degli esiti dell'utilizzo del Sistema S.A.R.I., qualora gli stessi si inseriscano in un più strutturato complesso di risultanze probatorie. In senso analogo, v. pure Cass., Sez. I, 6 maggio 2021, n. 36441, in *C.E.D. Cass.*, Rv. 282005; Cass., Sez. I, 21 luglio 2020, n. 21823, in *OneLegale*.

In altre occasioni ancora, la Corte, preferendo non avventurarsi in ordine alla valutazione sull'attendibilità del S.A.R.I, ha respinto le doglianze difensive relative al mancato utilizzo del *software* di riconoscimento facciale reputato maggiormente affidabile rispetto ai riconoscimenti effettuati *de visu*: cfr. Cass., Sez. IV, 14 marzo 2022, n. 8428, in *OneLegale*; Cass., Sez. IV, 27 settembre 2019, n. 39731, *ivi*.

diziaria, ci si deve interrogare sul possibile impiego di questa tecnologia nell'ambito dell'attività investigativa e sul terreno probatorio, e quindi sul suo possibile inquadramento giuridico.

La verifica sulla reperibilità nella disciplina processuale di disposizioni nelle quali incasellare i *tool* di riconoscimento facciale, oltre a rispondere all'ineludibile necessità di conformarsi al canone di legalità, è essenziale per stabilire quali impieghi sono compatibili con le limitazioni già dettate nell'*A.I. Act*[29] e nella legge-delega italiana recentemente approvata.

Si è suggerito di inquadrare talune funzioni del S.A.R.I., quanto meno nella versione *Enterprise*, nell'ambito delle attività di polizia giudiziaria volte all'identificazione dell'indagato *ex* art. 349 c.p.p.[30], e precisamente nell'ambito degli «altri accertamenti» ammessi dalla disposizione codicistica per finalità identificative (art. 349, co. 2 c.p.p.), svincolati dal rispetto di rigide forme prestabilite dal legislatore, e dunque realizzabili con qualsiasi metodologia, ivi incluse quelle che si servono dei dispositivi di A.I.[31].

Questa soluzione, peraltro, non è esente da profili critici[32]. Va sottolineato, infatti, che le attività indicate dall'art. 349, co. 2 c.p.p. sono in grado di raggiungere un notevole livello di invasività, essendo idonee a rilevare dati personali sensibili (biometrici e genetici): per questa ragione, il dato normativo postula la residualità delle operazioni maggiormente intrusive, ammettendo il ricorso a rilievi dattiloscopici, fotografici e antropometrici, nonché, per l'appunto, ad «altri accertamenti», solo «ove occorra», legittimandoli, quindi, soltanto qualora la persona rifiuti di fornire le proprie generalità o vi siano dubbi sulla veridicità delle dichiarazioni oppure sull'autenticità dei documenti di identificazione forniti.

Ora, se, per un verso, appare chiaro che il S.A.R.I., almeno nella variante *Enterprise*, è meno invasivo rispetto alle identificazioni effettuate mediante il prelievo coattivo di capelli o saliva (consentito dall'art. 349, co. 2-*bis* c.p.p.), dall'altro, «si amplifica il rischio che il sistema in questione metta in crisi la sussidiarietà postulata dall'art. 349, co. 2 c.p.p.: avendo la disponibilità di uno strumento di così agevole impiego come il S.A.R.I., è facile pronosticare la propensione degli inquirenti a servirsene, a discapito delle altre attività che –

[29] In questi termini, BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 170.

[30] In generale sull'art. 349 c.p.p., v., per tutti, BONTEMPELLI-MARCHESI, *sub* art. 349, in *Codice di procedura penale*[2], tomo I, a cura di Canzio-Bricchetti, Milano, 2024, 2796 ss.; PAULESU, *sub* art. 349, in *Codice di procedura penale commentato*[5], tomo II, a cura di Giarda-Spangher, Milano, 2023, 1678 ss.

[31] In tal senso, v. GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, 63; TORRE, *Intelligenza artificiale e indagini penali: prospettive future e garanzie di sistema*, cit., 1745.

[32] Su tali criticità, v. BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 171 s.

non richiedendo l'acquisizione di dati biometrici – risulterebbero meno invasive nella sfera personale dell'indagato»[33].

Di più. Potrebbe verificarsi anche un rischio opposto a quello appena descritto, ossia di sottoporre l'indagato a rilievi fotografici allo scopo di affidarli al responso del S.A.R.I. anche laddove non vi sia una reale incertezza sull'identità, così alimentando i già corposi *database* dei soggetti fotosegnalati. Rischio, peraltro, intensificato dalla novella normativa introdotta dall'art. 2, co. 8 L. 27 settembre 2021, n. 134 (c.d. «riforma Cartabia») che, escludendo la discrezionalità della polizia giudiziaria nell'esecuzione dei citati rilievi *ex* art. 349, co. 2 c.p.p., impone l'obbligo di effettuarli sempre nei confronti degli apolidi e di altri soggetti stranieri[34].

Il timore di eventuali usi arbitrari dei sistemi di riconoscimento facciale automatizzato appare tanto più fondato se si considera che l'identificazione rientra tra le attività investigative di iniziativa della polizia giudiziaria e, dunque, non è contemplato nemmeno un adeguato vaglio preventivo del pubblico ministero, il cui intervento è previsto soltanto in ipotesi circoscritte (ovvero quando bisogna procedere al prelievo coattivo di materiale biologico o all'accompagnamento dell'interessato presso gli uffici di polizia giudiziaria): la qual cosa collide con la previsione che delimita l'impiego dei sistemi di identificazione biometrica a quanto «strettamente necessario per le indagini», subordinandolo alla preventiva autorizzazione dell'autorità giudiziaria (artt. 5, par. 3, e 26, par. 10 Reg. 1689/2024)[35].

---

[33] Così BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 171, per il quale il pericolo di accordare «una corsia preferenziale» al sistema di riconoscimento facciale «s'intensifica laddove si consideri che questa pratica, potendo essere condotta senza il coinvolgimento dell'indagato» – quando, ad es., la polizia giudiziaria è già in possesso di una sua fotografia –, permetterebbe di mantenere il riserbo sull'indagine, evitando di innescare le garanzie prescritte dall'art. 349, co. 3 c.p.p.

[34] Tale rischio è segnalato sempre da BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 171 s. In ordine alla citata modifica apportata dalla «riforma Cartabia», cfr. DEI CAS, *Le nuove frontiere dell'identificazione personale, tra diritto processuale penale dello straniero e «cultura del controllo»*, in *Arch. pen. web*, 2024, 1, 1 ss.; DELLA RAGIONE, *Le nuove norme sull'identificazione*, in *La Riforma Cartabia. La prescrizione, l'improcedibilità e le altre norme immediatamente precettive*, a cura di Romano-Marandola, Pisa, 2022, 93 ss.; GIUNCHEDI, *Il codice univoco identificativo*, in *La giustizia penale dopo la c.d. Riforma Cartabia. Aggiornato alla legge 24 novembre 2023, n. 168 e al d.lgs. 19 marzo 2024, n. 31*, a cura di Geraci, Torino, 2024, 165 ss.; MAGGIO, *Apolidia e processo penale: nuove norme sulla identificazione dei* non cives, in *La riforma Cartabia. Codice penale – Codice di procedura penale – Giustizia riparativa*, a cura di Spangher, Pisa, 2022, 214 ss.; VARRASO, *La "nuova" identificazione dell'indagato-imputato apolide o proveniente da Paesi extra UE*, in *Dir. pen. proc.*, 2021, 1456 ss.

[35] In questi termini, BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 172 s.

È necessario, poi, vagliare l'ammissibilità dei sistemi di riconoscimento facciale a supporto dell'attività del pubblico ministero di individuazione di persone *ex* art. 361 c.p.p., ai fini della «immediata prosecuzione delle indagini»[36].
Così adoperato, lo strumento costituirebbe un formidabile ausilio per l'investigazione: tra gli svariati impieghi, a titolo esemplificativo, esso consentirebbe, nella modalità *Enterprise*, di individuare, a partire dalle immagini catturate dalle videocamere di sorveglianza presenti sulla *scena criminis*, le persone verso cui dirigere le indagini o che possono riferire circostanze utili per l'accertamento del fatto di reato e, nella versione *Real Time*, di affinare le ricerche nei luoghi pubblici dei soggetti indiziati, distinguendoli tra la folla.
Peraltro, l'ulteriore vantaggio del S.A.R.I. sarebbe quello di non subire l'inevitabile degradazione mnestica tipica della mente umana e di essere immune ai diversi fattori distorsivi – durata e contesto di osservazione, condizioni fisiologiche e psicologiche dell'osservatore, ecc. – che inevitabilmente influenzano il processo intellettivo con il quale una persona ne riconosce un'altra[37].
Adoperato per questi scopi, il programma di riconoscimento facciale sembrerebbe costituire una *species* tecnologicamente avanzata dell'attività disciplinata dall'art. 361 c.p.p.[38].
Tuttavia, anche questa strada non appare percorribile. La laconica regolamentazione offerta dall'art. 361 c.p.p., oltre ad essere del tutto incompatibile con i requisiti fissati dall'*A.I. Act* per contenere la straordinaria invasività dei sistemi che operano in *real time*, non soddisfa nemmeno le garanzie minime richieste, che impongono di contingentare l'uso di tutti i sistemi di identificazione biometrica a quanto strettamente necessario per le indagini (artt. 5, par. 3 e 26, par. 10 Reg, 1689/2024), nel rispetto del criterio di proporzionalità.
La disponibilità di un *software* dalle potenzialità così promettenti come il S.A.R.I., peraltro, rischierebbe di irrobustire la consolidata tendenza della giurisprudenza ad attribuire un'indebita valenza probatoria a un atto che, vi-

[36] Sull'individuazione di persone, in generale v., per tutti, GAETA-PICARDI, *sub* art. 361, in *Codice di procedura penale commentato*[5], a cura di Giarda-Spangher, cit., 1890 ss.
[37] Su tali fattori, cfr. GULOTTA-TUOSTO, *Il volto nell'investigazione e nel processo. Nuova Fisiognomica Forense*, Milano, 2017, 124 ss.; nonché, volendo, TRIGGIANI, *Ricognizioni mezzo di prova nel nuovo processo penale*, Milano, 1998, 263 ss.
[38] Cfr. LOPEZ, *La rappresentazione facciale tramite* software, cit., 253, secondo la quale il riconoscimento facciale sarebbe accostabile, seppur sotto forma di «filiazione spuria» all'individuazione *ex* art. 361 c.p.p.

ceversa, il dettato codicistico vorrebbe limitato soltanto alla «immediata prosecuzione delle indagini»[39].

Invero, «è l'idea stessa di servirsi del S.A.R.I. per le finalità indicate dall'art. 361 c.p.p. a non essere accoglibile a causa della natura 'artificiale' e non 'umana' del riconoscitore: l'individuazione effettuata dal *software* contrasta con il dato normativo di cui all'art. 361 c.p.p. che, invece, postula un soggetto ricognitore in 'carne ed ossa'»[40].

D'altronde, sarebbe «impensabile assimilare la capacità di un soggetto a fare un 'riconoscimento' con quella di un sistema algoritmico che punta a confrontare meccanicamente le caratteristiche dei volti», perché si rischierebbe «di confondere i processi della mente umana con quelli della macchina»[41]. Quest'ultima, «essendo incapace di riprodurre i processi neurologici e intuitivi umani, è addestrata per imparare a riconoscere le immagini a partire da un insieme di *pixel*, ricorrendo a inferenze statistiche elaborate su enormi quantità di dati; di conseguenza, il riconoscimento effettuato dal *tool* non è in alcuna misura accostabile all'attività indicata nell'art. 361 c.p.p. perché la comparazione eseguita dall'algoritmo segue logiche ed elabora dati totalmente differenti da quelli che entrano in gioco nell'ambito dell'individuazione per finalità investigative operata dall'uomo»[42].

È vero che è prevista una supervisione umana del risultato offerto dalla macchina, come si è più volte ricordato, attraverso un giudizio di compatibilità degli accoppiamenti, secondo un determinato coefficiente di probabilità, ma tale attività non trasforma in una valutazione umana il processo di elaborazione operato dal sistema.

---

[39] Il rilievo è di BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 174. In ordine alla tendenza della giurisprudenza ad attribuire valenza probatoria all'atto di individuazione, anche nel dibattimento, sia consentito rinviare a TRIGGIANI, *Ricognizioni mezzo di prova nel nuovo processo penale*, cit., 231 ss.

[40] Così BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 174.

[41] In questi termini, PALLANTE, *Le nuove sfide della cooperazione investigativa nello spazio europeo*, cit., 274. Nello stesso senso, BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 174, per il quale «sarebbe errato accostare le abilità dell'algoritmo alle capacità intellettive dell'uomo, stante la profonda differenza nel 'leggere' e confrontare le immagini facciali»; COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini,* cit., 128; GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, cit., 645 ss.; MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 42.

[42] BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 175.

Una volta accertata l'impossibilità di inquadrare il S.A.R.I. nei ricordati atti tipici della polizia giudiziaria e del pubblico ministero[43], bisogna verificare se sussistano i margini per incasellarlo nell'ambito delle indagini "atipiche"[44].
Anche questa opzione va, però, decisamente respinta, in quanto incompatibile con il paradigma delineato dall'art. 189 c.p.p. Tale norma – com'è noto – consente l'assunzione di "prove atipiche"[45], a condizione però che siano idonee all'accertamento del fatto di reato e non ledano la libertà morale della persona fonte di prova, e si ritiene, sia pure con qualche difficoltà, applicabile anche alla fase delle indagini preliminari.
Ora, le numerose incognite sui meccanismi di funzionamento dei *tool* di riconoscimento facciale costituiscono un ostacolo insormontabile per stabilirne l'attitudine epistemologica[46].
Il *match* restituito dal S.A.R.I. – al pari degli *output* prodotti dalla quasi totalità dei sistemi automatizzati di riconoscimento facciale – «scaturisce

[43] Come osserva BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 175, n. 98, va scartata anche l'opzione di inserire il S.A.R.I. nell'eterogenea categoria degli "accertamenti tecnici", in quanto la soluzione non offre alcuna garanzia né per quanto concerne la salvaguardia dei dati biometrici né, tanto meno, è rispettosa degli *standard* minimi richiesti dall'*A.I. Act* per fruire dei sistemi di identificazione biometrica; al contempo, va esclusa pure l'opzione di legittimare l'impiego degli strumenti in questione ampliando l'ambito operativo dei prelievi biologici coattivi di cui all'art. 359-*bis* c.p.p., in quanto, trattandosi di una disposizione relativa alla libertà personale e, dunque, di stretta interpretazione, non è suscettibile di letture analogiche (per ulteriori considerazioni su entrambi i profili appena considerati, v. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1083 ss.; MARANDOLA, *Il riconoscimento facciale*, cit., 512 s.).
Non è possibile neppure fare riferimento alla disciplina delle intercettazioni allo scopo di consentire l'uso della sorveglianza clandestina e contestuale realizzata dal S.A.R.I. *Real Time*, dal momento che "alla videoripresa con riconoscimento facciale manca del tutto la captazione di una comunicazione e, dunque, sulla base delle Sezioni Unite *Prisco,* non si può applicare per analogia la normativa sulle intercettazioni" (così GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., 63 s.).
[44] Sul tema delle indagini atipiche, cfr. diffusamente *Le indagini atipiche*[2], a cura di Scalfati, cit. Volendo, cfr. anche TRIGGIANI, *Legalità opaca, raccolta atipica e pre-investigazioni*, in *La procedura criminale. Quali riforme, Atti del Convegno – Web conferencing 22-23 ottobre 2020*, a cura di Maffeo, Roma-Perugia, 2021, 23 ss.
[45] In argomento, v., tra gli altri, C. CASTALDI, *La prova atipica nel processo penale*, Roma, 2025; C. CONTI, *sub* art. 189, in *Codice di procedura penale commentato*[5], a cura di Giarda-Spngher, tomo I, Milano, 2023, 2601 ss.; LARONGA, *Le prove atipiche nel processo penale*, Padova, 2002; TABASCO, *Prove non disciplinate dalla legge nel processo penale. Le "prove atipiche" tra teoria e prassi*, Napoli, 2011.
[46] In tal senso, v. BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 175; DI VIZIO, *L'intelligenza artificiale nelle attività di contrasto del terrorismo*, in *Intelligenza artificiale e indagini penali. Strumenti, garanzie, responsabilità e scenari dell'innovazione investigativa digitale*, a cura di Parodi-Rizzo, cit., 282 s.
Contra, TORRE, *Intelligenza artificiale e indagini penali: prospettive future e garanzie di sistema*, cit., 1747, per il quale non si profila alcun problema quanto alla idoneità probatoria degli strumenti in esame.

dall'autoapprendimento delle fittissime reti neurali dell'algoritmo, il quale, essendo addestrato con metodologie di *deep learning*, segue le impenetrabili modalità operative della *black box*»[47]. Risulta dunque inintellegibile la logica sottesa al processo decisionale della macchina, essendo impossibile, tanto per l'utilizzatore quanto per lo stesso programmatore comprendere e spiegare l'*iter* logico seguito dal *software* per addivenire a quello specifico risultato.

Peraltro, «la mancata trasparenza sul *set* di immagini adoperate per il *training* della macchina – oltre a rendere ancora più oscuri e incomprensibili i meccanismi sottesi al riconoscimento automatizzato – impedisce di verificare se l'operato del programma di A.I. è inficiato da *input* di partenza errati o poco rappresentativi»[48].

Si registrano diversi *bias* che ne intaccano l'attendibilità (si è, ad esempio, dimostrato come alcuni *tool*, essendo addestrati con *dataset* contenenti in prevalenza immagini di volti di uomini bianchi, sono inclini a compiere un maggior numero di riconoscimenti errati – c.d. "falsi positivi" – a discapito delle persone appartenenti a un'etnia diversa da quella caucasica)[49].

D'altra parte, proprio l'"opacità algoritmica" impedisce di fissare in termini assoluti e astratti il tasso di errore delle tecnologie di riconoscimento facciale, atteso che l'accuratezza e l'efficacia del sistema dipendono da una serie di variabili imprevedibili[50].

La concreta capacità dimostrativa dell'*output* restituito dal programma di A.I. è infatti influenzata da una serie di aspetti – qualità dell'immagine, grado di illuminazione, inclinazione e posa del volto, angolo di cattura dell'effigie facciale, età del soggetto, pettinatura, presenza di occhiali, trucchi o altri accesso-

---

[47] Cfr. BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 175; MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 52 ss.

[48] Così, ancora, BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 176. Come osserva MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 221, l'accuratezza del *software* potrebbe essere compromessa «e portare a risultati discriminatori se 'allenati' con dati storici che riflettono pregiudizi impliciti, o se le immagini campionate offrono una rappresentazione statisticamente distorta di gruppi rispetto al complesso della popolazione».

[49] Cfr., sul punto, LOPEZ, *Il riconoscimento facciale tramite* software, cit., 247.

[50] Non sono disponibili dati scientifici riguardo al tasso di errore del Sistema S.A.R.I. Ma alcuni studi hanno dimostrato la totale inaffidabilità dei sistemi di riconoscimento automatizzato del volto: in particolare – come ricorda DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 271 e n. 162 – una ricerca condotta da un'*equipe* dell'Università di Essex sul programma di riconoscimento facciale utilizzato dalla polizia londinese ha rilevato tassi di errore che si attestano sulla soglia dell'80%, per lo più dovuti a "falsi positivi".

In tema, v. BORGIA, *Profili sistematici delle tecnologie di riconoscimento facciale*, cit., 10; BORGIA-ZONARO, *L'errore nel riconoscimento facciale automatizzato*, in *L'errore tecnico e la prova penale*, a cura di Nocerino, Pisa, 2025, 175 ss.; GIALUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., 64.

ri – che condizionano il risultato finale, a seconda della soglia di sensibilità dello strumento preimpostata da chi addestra il sistema automatizzato[51]. In particolare, «più alta è questa soglia e maggiore la sensibilità del sistema, minore sarà il tasso di falsi-positivi (perché l'algoritmo, in ipotesi, tenderà a verificare che ci sia una più esatta coincidenza tra le immagini), ma maggiore sarà il tasso di falsi-negativi (perché in ipotesi, pur essendo le immagini raffiguranti la stessa persona, la diversità nelle rappresentazioni impedisce al sistema di ravvisare una coincidenza)»[52].

Dunque, non essendo conoscibile l'esatta procedura con la quale il *software* impara, in autonomia, a leggere e riconoscere i volti delle persone e, non avendo accesso al *dataset* con il quale è stato addestrato il dispositivo, è impossibile verificarne l'affidabilità e, quindi, stabilire se esso è idoneo ad assicurare l'accertamento dei fatti, come richiesto dall'art. 189 c.p.p.

Per quanto concerne, invece, l'altro requisito indicato dall'art. 189 c.p.p., l'impiego del S.A.R.I. *Real Time*, come potentissimo mezzo per sorvegliare in maniera continuativa e clandestina un numero potenzialmente infinito di persone, è incompatibile con la libertà morale *ex* art. 188 c.p.p.[53].

Al riguardo occorre sottolineare la straordinaria lesività dei *tool* che, operando in tempo reale e all'insaputa del soggetto interessato, monitorano chiunque transiti, anche soltanto casualmente, in un'area vigilata dalle telecamere munite di *software* di riconoscimento, benché del tutto estraneo alla vicenda sulla quale si sta indagando.

I sistemi di identificazione biometrica finiscono in verità per interferire con l'autonomia delle scelte individuali, in quanto sono in grado di realizzare un marcato *chilling effect* che induce le persone, proprio per il timore di essere soggette al trattamento biometrico, senza un loro espresso consenso o in luoghi dove non si aspettano di essere sorvegliate, a modificare le proprie abitudini, autolimitandosi nell'esercizio dei propri diritti fondamentali, come ad es.

---

[51] Sul punto cfr., tra gli altri, DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 14, 27 s., 105, 240 e 280.

[52] Così MOBILIO, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., 36.

[53] Cfr. BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 177; COLACURCI, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, cit., 122 ss.; DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1070; TORRE, *Intelligenza artificiale e indagini penali: prospettive future e garanzie di sistema*, cit., 1748.
In generale, sulla tutela della libertà morale *ex* art. 188 c.p.p. v., per tutti, CHELO, *La tutela della libertà morale nella formazione della prova penale*, Milano, 2025.

la libertà di riunione o di associazione, al fine di evitare le possibili conseguenze negative che potrebbero derivarne[54].

Del resto, la Corte europea dei diritti dell'uomo ha avuto occasione di sottolineare le pesanti ricadute prodotte sul diritto alla vita privata (art. 8 C.E.D.U.) in relazione alla raccolta e all'elaborazione delle immagini facciali di una massa indistinta di persone che transitano nel raggio di azione delle telecamere "intelligenti"[55]. Il monitoraggio occulto, capillare e prolungato nel tempo, sganciato da qualsivoglia limite e da garanzie adeguate a prevenire abusi, costituisce un serio attentato per i diritti individuali: sorvegliare in modo costante una platea generalizzata di soggetti che frequentano determinate aree, identificandoli in pochi secondi e a loro insaputa, pregiudica le libertà di espressione, di associarsi e riunirsi, permettendo di svelare una serie di informazioni inerenti alla sfera personale (ad es. convinzioni politiche, ideologiche, religiose).

Alla luce di tutto quanto già rilevato, a maggior ragione, non è possibile allo stato utilizzare i risultati ottenuti dai sistemi di riconoscimento facciale come prova in giudizio. L'ordinamento conosce un mezzo di prova tipico per il riconoscimento, puntualmente disciplinato dagli artt. 213 ss. c.p.p. ovvero la ricognizione di persona[56], e il riconoscimento automatizzato non è in alcun

---

[54] In tal senso v., tra gli altri, CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, in *Riv. it. dir. proc. pen.*, 2024, 249.

[55] Corte EDU, sez. III, 4 luglio 2023, *Gluckhin c. Russia*, in *Proc. pen. giust.*, 2024, 413 ss., con nota di BRUNO, *La condanna per manifestazione pacifica (non preavvisata e) con riconoscimento facciale viola i diritti fondamentali*.

A commento della decisione – che tra i precedenti maggiormente significativi richiama Corte EDU, 17 ottobre 2019, *López Ribalda e altri c. Spagna*, §§ 87-88 – v. altresì GALLO, *Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso* Gluckhin c. Russia *dinanzi alla Corte europea dei diritti dell'uomo*, in *MediaLaws*, 2023, 3, 189 ss.; MOBILIO, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento per reprimere il dissenso politico: osservazioni a partire dal caso* Gluckhin c. Russia, in *DPCE on line*, 2024, 1, 695 ss.; NARDOCCI, *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU* Gluckhin c. Russia, in *BioLaw Journal – Riv. BioDir.*, 2024, 1, 279 ss.

Nel caso di specie, la Corte, pur avendo riconosciuto che tale interferenza era dotata di una base giuridica nel diritto interno, ha stabilito che tuttavia non era fornita di norme adeguate e dettagliate tese a perimetrare, da un lato, l'ambito e l'applicazione delle misure che comportano l'uso delle tecnologie di riconoscimento facciale e, dall'altro, le relative garanzie contro il rischio di abusi e arbitrarietà. Ancorché, poi, l'obiettivo dell'interferenza possa considerarsi in astratto legittimo (perché finalizzato alla prevenzione del crimine), le misure adottate erano state ritenute particolarmente invasive (con particolare riferimento alla violazione dell'art. 8 C.E.D.U. accertata dalla Corte di Strasburgo, si vedano i §§ 58-91 della sentenza).

[56] Sulla ricognizione di persone, limitatamente ai lavori monografici, v. BERNASCONI, *La ricognizione di persone nel processo penale. Struttura e procedimento probatorio*, Torino, 2003; BONTEMPELLI, *La ricognizione nel processo penale*, Torino, 2012; CAPITTA, *Ricognizioni e individuazioni nel diritto delle prove penali*, Milano, 2001; CAVINI, *Le ricognizioni e i confronti*, Milano, 2015; CECANESE, *Confronto,*

modo equiparabile a tale mezzo di prova: nella ricognizione il ricognitore è un essere umano che abbia già in precedenza visto il soggetto da riconoscere e che, dopo averlo descritto e altri adempimenti preliminari, viene chiamato a riconoscerlo attraverso un esame comparativo tra almeno altri due soggetti a lui somiglianti, così da preservare l'atto da suggestioni o malizie, mentre nel riconoscimento automatizzato il ricognitore è una macchina, che "in tempo reale" o "in differita" emetterà un *match* di corrispondenza o non corrispondenza[57]. L'attività compiuta dai sistemi automatici di riconoscimento facciale «è condotta attraverso processi di trattamento, elaborazione e combinazione dei dati oggettivamente eterogenei da quelli che entrano in gioco nel corso della ricognizione disciplinata dalla legge»[58]. E l'intervento di un soggetto esperto che adopera la macchina o che ne supervisiona il risultato – in ossequio al principio "*human in the loop*" – non trasforma in un giudizio umano o in una valutazione esperta il risultato algoritmico. Non appare, quindi, possibile neppure veicolare i risultati del riconoscimento facciale attraverso la perizia e la consulenza tecnica, anche in considerazione dell'opacità algoritmica cui si accennava prima.

---

ricognizione ed esperimento giudiziale nella logica dei mezzi di prova, Napoli, 2013, spec. 67 ss.; nonché, volendo, TRIGGIANI, *Ricognizioni mezzo di prova nel nuovo processo penale*, cit.

[57] In tal senso, v. GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, cit., 647, secondo cui «l'attività epistemica condotta, in maniera automatizzata, dai *software* di riconoscimento facciale non [è] in alcun modo accostabile al riconoscimento compiuto dall'uomo», anche perché tali programmi, al pari di tutti gli applicativi basati sulla c.d. "intelligenza artificiale" tendono a riprodurre e velocizzare funzioni del cervello umano, ma non ne replicano – per quante somiglianze si possano ravvisare tra di esse – i processi e i meccanismi di funzionamento. Sulla necessità di tener distinto il riconoscimento facciale automatizzato dalla ricognizione di persona, v. pure DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 218 ss., 269 s. e 281, il quale esclude pure che il primo possa essere inquadrato nella pur discussa categoria, di creazione giurisprudenziale, delle c.d. ricognizioni atipiche o informali (222 s.).
Contra, SAPONARO, *Le nuove frontiere tecnologiche dell'individuazione personale*, cit., 3, secondo la quale la ricognizione personale *ex* art. 213 c.p.p., ma anche l'identificazione operata dalla polizia giudiziaria *ex* art. 349 c.p.p. o l'individuazione effettuata dal pubblico ministero *ex* art. 361 c.p.p., «quali metodi tradizionalmente utilizzati per il riconoscimento di un soggetto, vengono ora convertiti in strumenti di captazione tecnologicamente avanzati» facendo riferimento alle tecniche di riconoscimento facciale.

[58] Così, ancora, GALLUCCIO MEZIO, *Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*, cit., 647, il quale osserva: «Per risalire al dato ignoto (la corrispondenza o meno del volto) a partire da un dato noto (le due o più immagini poste in comparazione) il cervello umano ricorre a meccanismi molto complessi e in molti casi ancora sconosciuti ma, indubbiamente, eterogenei rispetto a quelli della macchina. Quest'ultima impiega in maniera automatizzata un coacervo di leggi scientifiche – quelle che governano la matematica, la statistica, l'informatica, l'intelligenza artificiale – che solo un sistema artificiale dotato di elevatissime capacità di calcolo è in grado di governare».

Escluso che il riconoscimento automatizzato possa essere ricondotto al modello legale della ricognizione di persona, data la diversità ontologica tra le due forme di riconoscimento, occorre valutare se possa rientrare tra le prove atipiche *ex* art. 189 c.p.p., in quanto prova fondata su una *novel science*: inquadramento possibile ove rispondesse ai requisiti di ammissibilità previsti da tale disposizione, che come già ricordato, esige che la prova atipica richiesta dalle parti sia idonea all'accertamento del fatto di reato e non lesiva della libertà morale della persona fonte di prova.

Al riguardo, si rinvengono, tuttavia, *a fortiori*, gli ostacoli già rappresentati con riferimento all'utilizzo di tali strumenti nel quadro delle indagini atipiche, ovvero la (attuale) carenza di idoneità epistemologica e di validità scientifica dei risultati emessi dai sistemi di riconoscimento facciale, in considerazione del già ricordato elevatissimo tasso di errore riscontrato (oltre che della lesione della libertà morale dell'individuo, quanto meno con riferimento alla modalità di funzionamento *real time*).

Nonostante tutte le criticità finora evidenziate, sul piano tecnico e giuridico, occorre in conclusione rilevare che risulterebbe ormai del tutto anacronistica una posizione di assoluta chiusura e preclusione nei confronti dell'utilizzo dei sistemi automatizzati di riconoscimento facciale: «il costante progresso nei settori di applicazione dell'intelligenza artificiale e dell'elaborazione delle immagini lascia presupporre che, nel prossimo futuro» tali sistemi «saranno in grado di eseguire comparazioni tra volti con un livello di accuratezza e affidabilità sempre più elevato»[59].

Insomma, i sistemi automatici di riconoscimento facciale, non soddisfacendo, allo stato, i requisiti che deve avere una "prova scientifica"[60] – in quanto non superano attualmente il "*Daubert test*" –, possono considerarsi una prova scientifica *in fieri.* Potranno diventare in futuro una prova scientifica: se sa-

[59] In questi termini, SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, cit., 262. Analogamente, DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 272, per il quale «è verosimile che, nel futuro prossimo, una ottimizzazione dei sistemi di riconoscimento facciale possa condurre verso un superamento del vaglio di idoneità della prova dell'accertamento del fatto», anche grazie «alla diffusione di videocamere in 3D». L'A. evidenzia però che «una identificazione univoca non possa realizzarsi neppure in futuro dato che i sistemi automatici di riconoscimento facciale risultano fortemente influenzati dalle modalità di funzionamento delle periferiche di *input* che, nei casi di riconoscimento facciale "in differita", nella stragrande maggioranza dei casi sono rappresentati dalle telecamere installate in luoghi pubblici o privati che, inevitabilmente, si differenziano per qualità degli obiettivi, dell'angolazione di ripresa e per qualità dell'immagine (anche al buio)».

[60] In argomento v., *ex multis*, *Prova scientifica e processo penale*[3], a cura di Canzio-Luparia Donati, cit.; *La prova scientifica*, a cura di Conti-Marandola, cit.; *La prova scientifica nel processo penale*, a cura di Carlizzi-Tuzet, Torino, 2018.

ranno raggiunti adeguati tassi di trasparenza, superando l'"opacità algoritmica" e rendendo note le modalità attraverso le quali l'algoritmo è generato; se sarà accertato che, in fase di programmazione, siano immessi dati sufficientemente rappresentativi e immuni da pregiudizi e condizionamenti; se sarà dimostrato il tasso di errore dell'algoritmo con riferimento ai "falsi negativi" e ai "falsi positivi"; se il procedimento di funzionamento dell'algoritmo sarà sottoposto a procedura di verificazione/falsificazione, secondo la nota teoria di Popper, e accettato dalla comunità scientifica di riferimento[61].

Intanto, appare quanto mai opportuno e urgente, alla luce di tutte le osservazioni sopra esposte, un intervento normativo compiuto, puntuale, rigoroso ed equilibrato, che – in attuazione del Reg. 1689/2024/UE e della L. 132/2025 (e in particolare di quanto previsto all'art. 24 di tale legge) – sia in grado di bilanciare in modo ragionevole e adeguato l'efficienza investigativa con la salvaguardia dei diritti fondamentali dell'individuo, garantendo il canone della proporzionalità, così da utilizzare tali sistemi nella fase delle indagini preliminari solo laddove risultino indispensabili, e assicurando la completa trasparenza delle loro modalità di funzionamento, al fine di poterne saggiare l'affidabilità dal punto di vista epistemologico e, al contempo, di preservarne la compatibilità con l'esercizio delle prerogative difensive[62].

[61] In tal senso, DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 280 s.

[62] In ordine a questo auspicio v., tra gli altri, con opportuni suggerimenti, BELVINI, *Intelligenza artificiale e circuito investigativo,* cit., 180 ss.; CAMALDO, *Intelligenza artificiale e investigazione penale predittiva*, cit., 249 s.; DEMARTIS, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, cit., 281 s.; SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, cit., 267 ss.