CONTRIBUTO DIVULGATIVO

L'identificazione biometrica remota in tempo reale e il nuovo art. 359-ter c.p.p. nel d.lgs. 160/2026

Manuela Davidde

Praticante Avvocato · Università degli Studi di Salerno

IDENTIFICATIVO
Contributo n. 12106
ISSN 2421-7123

LICENZA
CC BY-NC-ND 4.0

STORIA EDITORIALE
Pubblicato il 12 novembre 2026
Contributo divulgativo

COME CITARE
MANUELA DAVIDDE, *L'identificazione biometrica remota in tempo reale e il nuovo art. 359-ter c.p.p. nel d.lgs. 160/2026*, in Riv. Cammino Diritto, ISSN 2421-7123.

ABSTRACT

Il contributo esamina la disciplina dell'identificazione biometrica remota in tempo reale introdotta dal d.lgs. 9 settembre 2026, n. 160, con particolare riferimento al nuovo art. 359-ter c.p.p. L'analisi si sofferma sui presupposti che legittimano il ricorso a tali sistemi, sulle modalità autorizzative e sui meccanismi di controllo previsti, evidenziando il rapporto tra esigenze investigative e tutela dei diritti fondamentali.

The paper examines the regulation of real-time remote biometric identification introduced by Legislative Decree no. 160 of 9 September 2026, with particular reference to the new art. 359-ter of the Code of Criminal Procedure. The analysis focuses on the assumptions that legitimize the use of such systems, the authorization methods, and the control mechanisms envisaged, highlighting the relationship between investigative needs and the protection of fundamental rights.

SOMMARIO

1. Premessa e inquadramento sistematico 3
2. L'identificazione biometrica remota "in tempo reale": l'art. 8 3
3. Il nuovo art. 359- ter c.p.p. e i suoi riflessi nelle indagini preliminari 5
4. Profili da attenzionare: diritto alla privacy, risultato probatorio e diritto di difesa 6
4.1. L'art. 359- ter c.p.p. e il risultato probatorio 8
4.2. Identificazione biometrica e diritto di difesa 8
5. Riflessioni conclusive 9

1. Premessa e inquadramento sistematico.

Il 30 settembre 2026 è entrato in vigore il d.lgs. n. 160 del 2026[1] con il quale il Governo ha dato attuazione alle deleghe contenute nella legge 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale» consentendo l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2024/1689 (c.d. AI Act). Si è potuto così dare attuazione, sul versante nazionale, dell'art. 5, par. 5, del Regolamento di cui sopra, il quale rimette agli Stati membri la scelta di consentire, nel rispetto dei limiti e delle condizioni di cui al paragrafo 1, primo comma, lettera h) e ai paragrafi 2 e 3, l'impiego di sistemi di identificazione biometrica remota in tempo reale in luoghi accessibili al pubblico per finalità di contrasto. Tale facoltà presuppone l'introduzione, per l'appunto, di una disciplina nazionale volta ad individuare gli obiettivi perseguibili, le autorità legittimate a ricorrere a tali strumenti e le procedure per il rilascio e l'esercizio delle relative autorizzazioni, assicurando altresì adeguati meccanismi di controllo.

Si tratta di una manovra legislativa che ha consentito, senza la creazione di un ulteriore microsistema *extra* codicistico, di far confluire la disciplina nel codice di procedura penale attraverso l'introduzione del nuovo art. 359-*ter* (introdotto dall'art. 13 del decreto). L'intervento normativo trova fondamento nella delega conferita al Governo dall'art. 24, comma 5, lett. e), della legge 23 settembre 2025, n. 132, che prevedeva l'introduzione di una disciplina relativa all'impiego di sistemi di IA nelle indagini preliminari. Il legislatore delegante ha subordinato tale intervento al rispetto delle garanzie del diritto di difesa e della protezione dei dati personali dei terzi, chiedendo altresì che l'utilizzo di queste tecnologie fosse improntato ai principi di proporzionalità, non discriminazione e trasparenza. A tali vincoli si affianca il principio generale secondo il quale la normativa nazionale debba essere interpretata in conformità al Regolamento (UE) 2024/1689. Pertanto, la nuova disciplina deve essere letta alla luce di un quadro di principi volto a coniugare le esigenze investigative con la tutela dei diritti fondamentali.

In particolare, il d.lgs. n. 160 del 2026 fa riferimento all'utilizzo dei sistemi di intelligenza artificiale (in seguito IA) nell'ambito dell'attività di polizia (di cui al Titolo I) con disposizioni in materia di responsabilità civile e penale (Titolo II).

Il contributo si propone, dunque, di approfondire i principali profili della nuova disciplina esaminandone i presupposti applicativi, le garanzie procedurali e i meccanismi di controllo giurisdizionale, al fine di valutarne l'impatto sul sistema delle indagini preliminari e la coerenza con i principi di tutela dei diritti fondamentali.

2. L'identificazione biometrica remota "in tempo reale": l'art. 8

La prima novità la si rinviene nel Capo III, Titolo I, del d.lgs. 160 del 2026 il quale ammette l'utilizzo di sistemi di IA nell'ambito delle attività di polizia attraverso distinte tipologie di trattamento biometrico.

L'identificazione biometrica remota (IBR), di cui all'art. 3 dell'AI Act, mira ad identificare una persona fisica senza il suo coinvolgimento attivo, confrontando i dati biometrici ottenuti da uno specifico soggetto con i dati presenti nella banca dati di riferimento[2].

Più precisamente, si distinguono due tipologie di trattamento biometrico: l'identificazione biometrica remota "in tempo reale", finalizzata proprio alla ricerca di specifici soggetti, nonché alla prevenzione di

1. *Pubblicato in G.U. n. 214 del 15 settembre 2026*

2. *S. COMBA (2026), «Sorveglianza biometrica e partecipazione democratica: il parere del Garante Privacy e il decreto legislativo in tema di riconoscimento facciale nelle attività di polizia», in Annuario italiano dei diritti umani, 2026.*

attacchi terroristici o di minacce imminenti all'incolumità di persone fisiche; il riconoscimento facciale "a posteriori", finalizzato alla individuazione di soggetti sospetti di aver commesso un reato.

L'art. 8 del d.lgs. 160 del 2026 prevede l'utilizzo di sistemi di IA per l'identificazione biometrica remota in tempo reale in luoghi pubblici o aperti al pubblico da parte degli organi, uffici e comandi delle Forze di polizia solo per le finalità di prevenzione di cui all'art. 5, paragrafo 1, primo comma, lettera h), punto ii), del Regolamento (UE) 2024/1689, nonché per la ricerca di persone scomparse.

L'utilizzo dei sistemi di IA è consentito soltanto per confermare l'identità delle persone di cui al comma 1.

Il comma 3, art. 8, stabilisce, inoltre, che il confronto biometrico avviene esclusivamente con una banca dati "statica" adeguata in base all'esigenza e al soggetto da individuare. La banca dati utilizzata può avere al suo interno dati che sono in essa confluiti da altre banche dati in uso alle Forze di polizia o tenute da altre pubbliche amministrazioni, ovvero da immagini, filmati o altri elementi biometrici che siano stati acquisiti legalmente durante lo svolgimento delle attività di polizia. Ogni banca dati è costruita *ad hoc* per ciascuna autorizzazione e cancellata al termine della validità della stessa.

Così facendo si eviterebbe che i dati impiegati nelle singole operazioni siano progressivamente cumulati, attraverso il susseguirsi delle autorizzazioni, fino a costruire un archivio di riconoscimento biometrico di portata generale. La previsione appare condivisibile nella misura in cui circoscrive l'operazione di confronto entro limiti predeterminati, rafforzando la minimizzazione dei dati e contenendo il rischio di una sorveglianza sistematica degli individui.

La portata effettiva di tale garanzia dipenderà, tuttavia, dalle modalità con le quali si assicurerà l'attuazione. In tale prospettiva, assume particolare rilievo il decreto ministeriale di cui all'art. 9, comma 5, del medesimo decreto legislativo, cui è demandata la definizione dei requisiti tecnici delle banche dati di riferimento, delle misure di sicurezza e delle modalità di cancellazione[3]. Si noti come la garanzia legislativa richieda una adeguata specificazione tecnica e un sistema di controllo che sia idoneo ad assicurarne l'effettività.

Interessanti risultano i commi 4 e 5, art. 8, d.lgs. 160 del 2026 e il comma 6, dell'art. 359-ter c.p.p.: si noti come il legislatore abbia attribuito il potere autorizzatorio al procuratore della Repubblica, non già ad un giudice, stabilendo una durata massima dell'autorizzazione di quindici giorni, prorogabili e una clausola d'urgenza che consente l'attivazione del sistema da parte del questore o dei comandanti provinciali, subordinandola alla successiva convalida entro termini particolarmente stringenti.

La scelta di attribuire il potere autorizzatorio al pubblico ministero solleva interrogativi in merito al coordinamento della disciplina nazionale con l'art. 5, par. 3, dell'AI Act, il quale richiede che l'autorizzazione preventiva sia rilasciata da un'autorità giudiziaria oppure da un'autorità amministrativa indipendente la cui decisione sia vincolante.

Ora, sebbene la riconducibilità del pubblico ministero italiano alla nozione di autorità giudiziaria possa essere sostenuta alla luce della sua collocazione nell'ordinamento e delle garanzie di indipendenza che ne caratterizzano la figura, bisognerebbe verificare se il modello delineato dal legislatore nazionale assicuri, in concreto, un controllo preventivo che consenta una effettiva autonomia rispetto all'iniziativa delle Forza di polizia richiedenti, visto che si tratta delle stesse con le quali il procuratore coopera nelle indagini. Il problema, dunque, potrebbe sorgere in riferimento al coordinamento investigativo che intercorre tra p.m. e polizia giudiziaria.

L’art. 9 del d.lgs. 160 del 2026, invece, prevede per il titolare del trattamento di effettuare una valutazione preventiva di impatto sui diritti fondamentali (c.d. FRIA, acronimo di *Fundamental Rights Impact Assessment*), affiancata ad una valutazione di impatto sulla protezione dei dati personali (c.d. *Data Protection Impact Assessment*), ai sensi degli artt. 23 e 24, d.lgs. 18 maggio 2018, n. 51.

Successivamente all’utilizzo dei suddetti sistemi di IA, il titolare del trattamento deve effettuare notifica al Garante. Essa contiene tutte le informazioni essenziali per l’autorizzazione rilasciata e sul risultato conseguito attraverso l’utilizzo del sistema.

3. Il nuovo art. 359-*ter* c.p.p. e i suoi riflessi nelle indagini preliminari

Il d.lgs. 160 del 2026, all’art. 13, ha introdotto nel codice di procedura penale l’art. 359-*ter*. La nuova disposizione, rubricata «Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale», disciplina l’utilizzo di sistemi di IA per l'identificazione biometrica remota in tempo reale da parte dell’autorità giudiziaria e della p.g., quando occorre confermare l’identificazione di una persona che si ritiene aver commesso uno dei delitti previsti all'allegato II del Regolamento (UE) 2024/1689, punibile con la pena della reclusione non inferiore nel massimo a quattro anni; quando occorre procedere alla ricerca di un latitante ai fini della applicazione e dell’esecuzione di una misura cautelare; per la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani.

Si può notare che la previsione dell’entità del massimo edittale (comma 1), mira a garantire l’utilizzo di tali sistemi di IA, in presenza di un reato definito sufficientemente grave da giustificarne l’impiego.

La nuova disposizione va così a colmare un vuoto normativo divenuto sempre più evidente in ragione di una rapida evoluzione tecnologica e della conseguente necessità di adeguare il quadro giuridico alle nuove possibilità offerte dagli strumenti di IA nello svolgimento delle indagini preliminari.

Precedentemente, infatti, l’identificazione biometrica non trovava alcuna tipizzazione all’interno del codice di rito. Le attività investigative in materia di acquisizione dei dati biometrici si svolgevano in un contesto normativo caratterizzato da margini di incertezza, riconducibili alle attività previste all’art. 348 c.p.p. da parte della p.g., agli accertamenti tecnici non ripetibili di cui all’art. 360 c.p.p., nonché l’identificazione così come prevista dagli artt. 349 c.p.p. e art. 4 t.u.p.s., la prima legata alle indagini esplicata dalla polizia giudiziaria, la seconda con carattere preventivo effettuata dalla polizia di sicurezza.

Così come delineato, il quadro normativo si basava sull’art. 10 della direttiva (UE) 2016/680 e, da un punto di vista nazionale, dal d.lgs. n.51/2018, con controlli demandati in un secondo momento al Garante. L’AI Act, invece, ha introdotto una disciplina speciale e più specifica, stabilendo, nei limiti e con le eccezioni da esso previste, la prevalenza delle proprie disposizioni rispetto alla disciplina generale del trattamento dei dati biometrici *ex* art. 10 della direttiva (UE) 2016/680.

Il legislatore, così facendo, ha inteso definire un quadro normativo unitario per l’utilizzo delle tecnologie interessate e per il conseguente trattamento dei dati biometrici, riducendo quindi le incertezze interpretative derivanti dalla precedente sovrapposizione delle disposizioni.

Procedendo all’analisi del nuovo art. 359-ter c.p.p., risulta di particolare rilievo la riserva di giurisdizione di cui al comma 6, per cui per l’utilizzo di tali sistemi di IA e di identificazione biometrica remota in tempo reale, il pubblico ministero richiede l’autorizzazione al giudice per le indagini preliminari. Questa ultima deve contenere l’area geografica di applicazione, indicazione delle persone specifiche ricercate e deve essere indicato il tempo strettamente necessario che non può superare i

3. *V. FRA, Remote Biometric Identification for Law Enforcement Purposes: Fundamental Rights Implications, Vienna, 2026.*

quindici giorni (prorogabili dal giudice per altri quindici giorni), con possibilità di procedere anche in casi di urgenza sottoposta a convalida. Tale scelta, contemplata dall'art. 5, par. 3, dell'AI Act, rispecchia le garanzie che caratterizzano il sistema processuale penale italiano, nel quale le attività investigative che spesso possono incidere sui diritti fondamentali, sono assoggettate a specifiche forme di controllo giurisdizionale, si pensi agli artt. 266 ss., c.p.p.

Il comma 7 della norma in esame prevede una procedura eccezionale e accelerata per l'attivazione dell'identificazione biometrica remota in tempo reale mediante sistemi di IA, quando sussistono ragioni di urgenza tali da non consentire di seguire l'iter ordinario. Più specificamente: quando vi sono ragioni di urgenza e il ritardo rischia di provocare un pregiudizio grave e irreparabile alle finalità investigative previste dai commi precedenti, il p.m. dispone con decreto l'utilizzo del sistema, nel rispetto delle indicazioni di cui al comma 6. Il decreto deve essere immediatamente comunicato e comunque non oltre le ventiquattro ore al g.i.p., il quale, se ricorrono i presupposti, nelle successive quarantotto ore convalida il provvedimento e autorizza la prosecuzione.

Nelle stesse ipotesi di cui sopra, se non è possibile attendere il provvedimento del p.m., all'attivazione del sistema di IA per l'identificazione biometrica remota in tempo reale provvedono gli ufficiali di p.g. Entro le dodici ore dalla attivazione, deve essere trasmessa al p.m. la richiesta di autorizzazione, il quale, se sussistono i presupposti, richiede al g.i.p. la convalida entro ventiquattro ore dall'avvio del sistema.

L'art. 359-ter, comma 3, c.p.p., prevede l'utilizzo «di una banca di riferimento adeguata per ciascuna delle finalità di cui ai medesimi commi, contenente i dati biometrici e le relative informazioni identificative, ove disponibili, riferiti alle persone, anche non identificate, di cui ai medesimi commi 1 e 2.» La norma, dunque, si pone in una posizione di conformità rispetto alla previsione di cui all'art. 5, par. 1, lett. e), del Regolamento (UE) 2024/1689 il quale prevede il divieto dell'utilizzo di sistemi IA volti a creare o ampliare banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso.

L'art. 14 del d.lgs. 160 del 2026, rubricato «modifica alle norme di attuazione, di coordinamento e transitorie del codice di procedura», invece, ha previsto all'art 104, comma 1, delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale di cui all'allegato al d.lgs. 271/1989, la sostituzione delle parole «del profilo personale» con «generati anche con sistemi di intelligenza artificiale». Tale previsione prende atto della inevitabile (ormai) presenza di contenuti sintetici come immagini, registrazioni audio e video, nel materiale acquisito in un procedimento penale. In tale prospettiva assume rilievo più recente giurisprudenza, attraverso la quale la Sesta Sezione della Corte di cassazione ha affrontato il tema delle perizie foniche mediante *software* basate sulla IA, precisando che una nuova valutazione tecnico-scientifica di elementi già noti può integrare una «prova nuova» *ex* art. 630, comma 1, lett. c), c.p.p., qualora l'impiego di metodologie più evolute permette di individuare dati obiettivi precedentemente non rilevanti, suscettibili di condurre ad una differente valutazione dei fatti[4].

4. Profili da attenzionare: diritto alla privacy, risultato probatorio e diritto di difesa.

Quando ci si approccia a temi riconducibili all'utilizzo di IA, una prima perplessità sorge in riferimento al trattamento dei dati personali.

Vita privata, domicilio, corrispondenza, sono termini ai quali è da sempre associata una particolare, per così dire, sacralità[5].

4. *Cass. Sez. VI, n. 29015 del 30 luglio 2026*

5. *Così, S. PIETROPAOLI, Privacy e oblio. La protezione giuridica dei dati personali, in Scienza giuridica e tecnologie informatiche, Torino, Giappichelli, 2017, pp. 41 ss.*

In Italia il primo atto normativo con cui si è tentato di dare ordine alla materia della protezione dei dati personali e di conformarsi alla direttiva 95/46/CE è stata la legge 31 dicembre 1996, n. 675, sostituita poi dal c.d. "Codice privacy" (d.lgs. 196 del 2003).

La legge n. 675 del 1996 è stata fondamentale per aver istituito l'autorità Garante, figura che svolge un ruolo centrale nell'assicurare una tutela effettiva della *data privacy*[6].

Come si può intuire la tematica è di grande rilevanza, si tratta di una disciplina che ha avuto una sua particolare evoluzione fino ad arrivare ad oggi, con il d.lgs. 160 del 2026 che ha introdotto i sistemi di identificazione biometrica remota in tempo reale. L'utilizzo di questi sistemi, infatti, impone una riflessione sul rapporto che intercorre tra le esigenze investigative e la tutela della vita privata, la quale non può ritenersi recessiva per il solo fatto che l'attività di identificazione si svolga in luoghi accessibili al pubblico. La possibilità di rilevare e confrontare tratti biometrici delle persone, anche in assenza di una loro partecipazione consapevole, potrebbe determinare una interferenza con la sfera individuale che non riguarda solo la riservatezza, ma anche il diritto alla protezione dei dati personali. È necessario, quindi, che il ricorso a tali strumenti sia circoscritto a finalità tassativamente individuate. In tale prospettiva la disciplina introdotta dal nuovo d.lgs. 160 del 2026 deve essere letta alla luce degli artt. 7 e 8 della Carta di Nizza, dell'art. 8 CEDU e delle disposizioni del Regolamento (UE) 2024/1689.

Nel quadro appena delineato, si inserisce il parere del Garante della *privacy* del 14 luglio del 2026, nel quale, allo schema del decreto, ha ritenuto opportune alcune modifiche volte a rafforzare le garanzie in materia di trattamento dei dati personali. Prima del testo definitivo, si è richiesta la modifica dell'art.10: secondo il Garante il trattamento automatico dei dati biometrici di tutte le persone che accedono a luoghi o eventi designati non era conforme all'art. 26 dell'AI Act. Per tale ragione, il Garante ha richiesto (per la versione definitiva del decreto) che il trattamento biometrico non avvenisse in modo automatico al momento della registrazione del filmato, ma soltanto in un secondo momento, sul materiale registrato, qualora emerga una specifica esigenza operativa.

Il parere del Garante sollecita a una riflessione: il riconoscimento facciale, rischia di trasformare la partecipazione agli eventi pubblici in un'attività identificabile e tracciabile. Una persona che partecipa ad una protesta, infatti, si aspetta di essere vista, ma non di essere identificata, registrata in una banca dati e rintracciata eventualmente in futuro. Il punto centrale, dunque, è che la identificazione biometrica non incide soltanto sulla riservatezza, ma può scoraggiare le persone dall'esercitare liberamente i propri diritti in una società democratica. Si pensi al diritto di riunione previsto dall'art. 17 Cost.

In tale prospettiva, la tutela dei diritti inviolabili costituzionalmente tutelati fa da *pendant* alla disciplina dell'identificazione biometrica, orientandone l'interpretazione e delimitandone l'ambito di applicazione. Si pensi agli artt. 13 (diritto alla libertà personale), art. 14 (diritto all'intimità domiciliare) e l'art. 15 (diritto alla libertà e alla segretezza delle comunicazioni) Cost.: la violazione di queste norme non è consentita se non per atto motivato dalla autorità giudiziaria e nei soli casi e nei modi previsti dalla legge. L'utilizzo delle nuove tecnologie, nonché dei sistemi di IA, si pensi anche al Trojan Horse, vanno inevitabilmente ad incidere su tali diritti, tuttavia, si potrebbe ai fini della trattazione riprendere un passaggio della giurisprudenza prevalente delle Sezioni Unite secondo le quali l'utilizzo di questi mezzi debba essere posto «in ordine alla necessità del ricorso allo strumento informatico»[7].

6. *All'art. 4 il Codice della privacy detta una vera e proprio "grammatica" essenziale della privacy, definendo soggetti e oggetti della disciplina. Così, PIETROPAOLI, op.cit.*

7. *Cass. Pen., Sez. un., 28 aprile 2016, n. 26889*

4.1. L’art. 359-*ter* c.p.p. e il risultato probatorio

Il nuovo art. 359-ter, comma 8, c.p.p. si riferisce espressamente ai «risultati forniti dai sistemi di intelligenza artificiale» e ne sancisce l’inutilizzabilità quando il sistema sia stato impiegato fuori dei casi consentiti dalla legge o siano state violate le prescrizioni dei commi 6 e 7. La domanda da porsi è dunque se il risultato dell’identificazione biometrica possa essere ricondotto a una categoria probatoria già disciplinata dal codice oppure se presenti caratteristiche tali da richiedere una riflessione sull’art. 189 c.p.p.

Guardando alla previsione di cui all’art. 359-ter c.p.p., la corrispondenza biometrica restituita dal sistema, ossia il risultato del confronto tra il volto rilevato e i dati presenti nella banca dati di riferimento, potrebbe essere considerata un elemento probatorio a formazione algoritmica[8].

L’identificazione della persona come risultato dell’attività investigativa, può invece assumere rilievo come dato utilizzabile per orientare le indagini e , nei limiti previsti dalla legge, concorrere alla ricostruzione del fatto.

Le immagini e le registrazioni dalle quali si ricavano i dati biometrici possono essere riconducibili a categorie probatorie tipiche, secondo le modalità della loro acquisizione.

4.2. Identificazione biometrica e diritto di difesa

Nel caso dell’identificazione biometrica remota in tempo reale, il diritto di difesa assume una particolare rilevanza, poiché l’impiego di sistemi di intelligenza artificiale introduce una modalità di acquisizione di informazioni investigative caratterizzata da un procedimento tecnico e algoritmico che non sempre è immediatamente conoscibile dalle parti. Qui la questione investe soprattutto la concreta possibilità di verificarne l’attendibilità, ricostruire le modalità attraverso le quali è stato prodotto e contestare eventuali errori o anomalie.

La circostanza che un algoritmo abbia individuato una corrispondenza tra il volto rilevato e quello presente in una banca dati non consente, infatti, di considerare automaticamente certa l’identificazione. Per tali ragioni e anche in tali casi è sempre riconosciuto il diritto di difesa.

Tale esigenza trova il suo fondamento anzitutto nell’art. 24 Cost., il quale garantisce il diritto di difesa in ogni stato e grado del procedimento, e nell’art. 111 Cost., il quale, oltre a sancire il principio del contraddittorio, riconosce all’accusato il diritto di disporre delle condizioni necessarie per preparare la propria difesa. Rileva altresì l’art. 6, par. 3, lett. b) e d), CEDU, che garantisce il tempo e le facilitazioni necessarie per preparare la difesa.

Si tratta di garanzie che, pur non essendo previste specificamente riguardo all’identificazione biometrica remota in tempo reale, costituiscono certamente il perimetro entro il quale muoversi per valutare l’effettività della contestazione dei risultati tecnologicamente elaborati.

Si noti, inoltre, che il trattamento dei dati personali effettuato dalle autorità competenti per finalità di prevenzione, indagine, accertamento e perseguimento dei reati è disciplinato dalla direttiva (UE) 2016/680 e, nell'ordinamento interno, dal d.lgs. 18 maggio 2018, n. 51. In tale ambito, l'art. 8 del decreto legislativo vieta, salvo specifiche deroghe previste dalla legge e assistite da adeguate garanzie, le decisioni basate unicamente su trattamento automatizzato, compresa la profilazione, volti a produrre effetti negativi nei confronti dell'interessato. Tuttavia, la disposizione non esclude l'utilizzo di sistemi di IA a supporto delle attività investigative.

8. *S. SALVATORE, Valutazione e mediazione algoritmica, in ID, Decisioni algoritmiche e diritto, Milano, Giuffrè Lefebre, 2024, p. 53 ss.*

A tal proposito, infatti, si noti come il nuovo art. 359-*ter* c.p.p. non determina espressamente le modalità attraverso le quali la difesa possa accedere alle informazioni tecniche necessarie per la contestazione. Tuttavia, non è un caso che l'art. 9, comma 2, del d.lgs. n. 160 del 2026, imponga la registrazione automatica di ogni utilizzo del sistema mediante appositi file log non modificabili e conservati per cinque anni. Naturalmente, restano rilevanti anche gli strumenti di investigazione difensiva previsti dagli artt. 327-*bis* e 391-*bis* e ss. c.p.p., nonché la facoltà di avvalersi di consulenti tecnici *ex* art. 233 c.p.p.

Ne consegue, ancor di più, la totale centralità del contraddittorio: la sua funzione non è soltanto quella di consentire la contestazione dell'identità attribuita dal sistema, ma anche quella di sottoporre a verifica il procedimento tecnologico attraverso il quale tale attribuzione è stata effettuata.

5. Riflessioni conclusive

L' identificazione biometrica remota in tempo reale introdotta nel procedimento penale, rappresenta un significativo sviluppo delle tecniche investigative destinato ad incidere sulle modalità di acquisizione delle informazioni e di individuazione dei soggetti coinvolti nella commissione dei reati. La disciplina introdotta dal d.lgs. n. 160 del 2026, costituisce un primo tentativo di ricondurre l'impiego di tali strumenti entro un quadro normativo specifico, definendone i presupposti, le finalità e le garanzie.

La riforma incide significativamente nel processo di integrazione del progresso tecnologico nell'amministrazione della giustizia, palesando la volontà del legislatore interno di trasformare le potenzialità dell'intelligenza artificiale in strumenti concretamente funzionali all'efficacia dell'accertamento penale.

Come già evidenziato, tale manovra legislativa abbraccia il lavoro svolto dal legislatore europeo il cui obiettivo resta la protezione dei diritti e delle libertà fondamentali delle persone fisiche, attraverso una attenta regolamentazione dell'applicazione delle nuove tecnologie[9].

La strada intrapresa con l'ausilio dell' IA porterà alla formazione di elementi di prova sempre più dettagliati volti a dimostrare la colpevolezza o l'innocenza dell'imputato[10].

Il tema qui affrontato si presta ad una riflessione di più ampio respiro: l'adozione di strumenti basati sull'IA appare una scelta inevitabile per un ordinamento chiamato a confrontarsi con un progresso tecnologico sempre più rapido e pervasivo. La necessità di adeguare il sistema giuridico alle nuove realtà tecnologiche non riguarda soltanto l'attività investigativa e giudiziaria, ma investe l'intero mondo delle professioni legali, coinvolgendo avvocati, magistrati e studiosi del diritto. L'intelligenza artificiale può certamente offrire un contributo significativo favorendo una maggiore efficienza nello svolgimento delle attività professionali.

In conclusione, ne deriva che l'IA debba essere concepita non già come un sostituto del sapere giuridico e della valutazione umana, bensì come uno strumento di supporto da utilizzare con consapevolezza, competenza e senso critico. Soltanto attraverso un impiego responsabile, accompagnato da adeguate verifiche e da una costante supervisione umana, sarà possibile valorizzare in concreto i benefici senza compromettere le garanzie che costituiscono il fondamento dello Stato di diritto.

Naturalmente, il tema affrontato è di recente emersione, che apre indubbiamente prospettive di indagine inedite. I profili su cui ci si è soffermati e le riflessioni presentate si collocano in una prospettiva *de iure condendo* guardando anche agli interventi legislativi che ci saranno da qui all'avvenire.

9. *Cfr. Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016; d.lgs. 18 maggio 2018, n. 51, art. 8.*

10. *V. M. VIGGIANO, L'intelligenza artificiale e l'elemento di prova del futuro, in Iura e Legal Systems, XI, 2024, P. 1 ss.*