

ATTUALITÀ

BRUNA CAPPARELLI

Il deficit di conoscibilità dell'identificazione biometrica remota in tempo reale nel nuovo art. 359-ter c.p.p.

Il nuovo art. 359-ter c.p.p., introdotto in attuazione del regolamento (UE) 2024/1689, commina l'inutilizzabilità dei risultati dell'identificazione biometrica remota illegittimamente impiegata, ma non predispone la sequenza processuale – documentazione, deposito, accesso difensivo – attraverso la quale il fatto generatore della sanzione divenga conoscibile alla parte che dovrebbe dedurla e al giudice che dovrebbe rilevarla. Il contributo indaga la dissociazione così prodotta fra esistenza e azionabilità del divieto probatorio, verificandone la tenuta attraverso una controprova interna al medesimo decreto, che per l'azione risarcitoria costruisce un accesso tipizzato alla documentazione tecnica, e attraverso il raffronto con i modelli codicistici. Ne emerge un vizio di costruzione della fattispecie.

An unenforceable exclusionary rule: real-time remote biometric identification under the new article 359-ter of the Italian code of criminal procedure

The new Article 359-ter of the Italian Code of Criminal Procedure, enacted to implement Regulation (EU) 2024/1689, excludes evidence obtained through the unlawful use of real-time remote biometric identification, yet establishes no procedural sequence – recording, filing, defence access – whereby the fact triggering exclusion may become known to the party who should raise it and to the judge who should apply it ex officio. The article examines the resulting severance between the existence and the enforceability of the exclusionary rule, testing its thesis against a counterproof internal to the decree itself, which affords civil claimants typified access to technical documentation, and against the codified models. A defect in the construction of the provision emerges.

SOMMARIO: 1. Delimitazione del tema. – 2. La struttura della sanzione processuale. – 3. Il presupposto tacito dell'inutilizzabilità: la notizia dell'atto. – 4. Ciò che la disciplina produce, e a chi è destinato. – 5. Una controprova interna al decreto. – 6. Il raffronto con i modelli codicistici, con la disciplina parallela e con le esperienze straniere. – 7. Il piano della delega e quello convenzionale. – 8. Ipotesi ricostruttive. – 9. Rilievo conclusivo.

1. *Delimitazione del tema.* Fra le disposizioni di più immediato rilievo processuale contenute nel decreto legislativo di adeguamento della normativa nazionale al regolamento (UE) 2024/1689 in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale si colloca quella che il legislatore delegato ha inserito, dopo l'art. 359-bis c.p.p., sotto la rubrica «Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale»: l'art. 359-ter c.p.p.¹. Sulla norma si sono già appuntati rilievi critici di non poco mo-

¹Il riferimento è al d.lgs. 9 settembre 2026, n. 160, pubblicato nella *Gazzetta ufficiale* del 15 settembre 2026, n. 214, ed entrato in vigore il 30 settembre 2026, il cui art. 13 inserisce nel codice di procedura penale, dopo l'art. 359-bis, il nuovo art. 359-ter. Il provvedimento è stato approvato in esame preliminare dal Consiglio dei ministri il 10 giugno 2026 e trasmesso alle Camere il 24 giugno 2026 (atto del Governo n. 418), sul quale sono stati resi i pareri del Garante per la protezione dei dati personali (prov.

mento, concernenti la collocazione sistematica, l'assetto del procedimento autorizzativo e, segnatamente, i poteri riconosciuti alla polizia giudiziaria nei casi di urgenza².

A quei profili non si tornerà. Le pagine che seguono muovono da un angolo visuale diverso: il rapporto fra la sanzione processuale del co. 8 e il regime di conoscibilità dell'attività cui essa accede. Che l'impiego di strumenti algoritmici nell'accertamento penale sollevi un problema di trasparenza, di verificabilità e di controllo difensivo è, beninteso, acquisizione risalente e largamente condivisa, in Italia come altrove³. Meno esplorato appare il modo in cui quel problema si atteggia una volta che il legislatore delegato abbia scelto di presi-

14 luglio 2026, n. 531), della Conferenza unificata (rep. atti n. 87/CU del 20 luglio 2026) e delle Commissioni parlamentari; l'approvazione definitiva è intervenuta nella seduta del 4 agosto 2026. Nella versione licenziata il 10 giugno la disposizione figurava all'art. 15 dello schema.

²V. GIALUZ, *Riconoscimento biometrico e garanzie necessarie nello Stato democratico*, in *Sistema penale*, 30 luglio 2026, rielaborazione della memoria depositata in occasione dell'audizione presso la Commissione giustizia della Camera dei deputati del 23 luglio 2026, ove si propone di ricollocare la materia in un nuovo Capo IV-bis del Titolo III del Libro III del codice e si prospetta l'illegittimità costituzionale, per violazione dell'art. 3 Cost., della facoltà di attivazione autonoma riconosciuta agli ufficiali di polizia giudiziaria dal co. 7. Nella medesima direzione, in sede di osservazioni allo schema, la nota dell'Unione delle camere penali italiane del luglio 2026.

³Cfr. DELLA TORRE, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, p. 1057 ss.; BILIGOTTI, *Frizioni costituzionali nell'era della sorveglianza: intelligenza artificiale, processo penale e identificazione biometrica*, in *MediaLaws - Riv. dir. media*, 2022, il quale già rilevava che le esigenze del giusto processo impongono la *discovery* dei dati rilevanti in favore dell'accusato, estesa alla qualità dell'algoritmo, alla banca dati di riferimento e al tasso di errore; SACCHETTO, *Tecnologie di riconoscimento facciale e procedimento penale. Indagine sui fondamenti e sui limiti dell'impiego della biometria moderna*, Torino, 2025; e, sulla categoria dei controlli occulti e continuativi, NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria*, Milano, 2020. Quanto al nesso fra opacità algoritmica e prerogative difensive, GIALUZ, *Prove fondate sull'intelligenza artificiale e diritti fondamentali*, in *Diritto di difesa*, 15 gennaio 2025, che, muovendo dai canoni enunciati da Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, valorizza il «principio di conoscibilità» dei processi decisionali automatizzati e osserva come l'impresa che metta il sistema a disposizione dell'autorità ne accetti le conseguenze in termini di *discovery*; GALGANI, *Il legislatore italiano dinanzi all'IA nel c.d. «dominio Giustizia»*, in *Questione giustizia*, n. 3/2026, p. 67 ss., spec. pp. 80-81, secondo cui l'interessato e la sua difesa devono disporre di una «chance concreta» di sindacare gli esiti dei sistemi impiegati, e per la quale i contenuti del decreto ministeriale di cui all'art. 9, co. 5, potrebbero costituire il «dossier» tecnico su cui esercitare un controllo difensivo non meramente simbolico. Nella letteratura straniera, con specifico riguardo all'accesso difensivo ai risultati del riconoscimento facciale, BARRANCO, *Match Up: Increasing Disclosure of Facial Recognition Technology With Criminal Discovery Rules*, in *Duke Journal of Constitutional Law & Public Policy*, vol. 18, 2023, p. 135 ss. Il presente contributo si colloca a valle di questa elaborazione e ne assume gli esiti: il rilievo che segue non concerne la trasparenza dell'algoritmo, ma la struttura di una sanzione processuale il cui presupposto applicativo non è reso conoscibile.

diare l'illegalità dell'impiego con una specifica sanzione probatoria: se, cioè, alla sanzione si accompagna la sequenza processuale attraverso la quale il fatto che la genera divenga conoscibile alla parte che dovrebbe dedurla e al giudice che dovrebbe rilevarla. Guardata da questo lato, la disposizione lascia scoperto un passaggio che si direbbe indispensabile, giacché il divieto probatorio ivi comminato postula, per poter essere fatto valere, una conoscenza che la fattispecie non è congegnata ad assicurare. Se l'esito sia stato voluto o soltanto non avvertito è interrogativo che non occorre sciogliere; conviene semmai osservare fin d'ora che esso non trova giustificazione in difficoltà di ordine tecnico, come è dato ricavare dal medesimo provvedimento.

2. *La struttura della sanzione processuale.* Il co. 8 dell'art. 359-ter stabilisce che i risultati forniti dai sistemi di intelligenza artificiale non possono essere utilizzati qualora gli stessi siano stati impiegati fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dai co. 6 e 7; e aggiunge che, in tali casi, tutti i dati personali, i risultati e gli *output* acquisiti e prodotti sono cancellati, salvo che costituiscano corpo del reato⁴.

La relazione illustrativa qualifica la previsione come formulata «secondo il paradigma dell'art. 191 c.p.p.» e la descrive quale «strumento di chiusura del sistema di garanzie». La qualificazione è corretta quanto alla struttura: si tratta di una inutilizzabilità speciale, ancorata alla violazione di un divieto legale di acquisizione, e come tale rilevabile anche d'ufficio in ogni stato e grado del procedimento ai sensi dell'art. 191, co. 2 c.p.p. Meno persuasiva è la seconda proposizione, che attribuisce alla norma un'efficacia di chiusura. Una regola di chiusura tale è in quanto opera; e una regola probatoria opera in quanto esista una parte in condizione di dedurre la violazione o un giudice in condizione di rilevarla.

Conviene precisare l'oggetto del divieto. Esso non investe l'atto nella sua interezza, ma il suo esito: i «risultati forniti» dal sistema, ossia l'informazione identificativa o localizzativa prodotta dal confronto biometrico. Restano fuori dal perimetro esplicito della sanzione gli elementi che da quel risultato derivano: l'arresto eseguito sulla scorta della localizzazione, la perquisizione che ne è conseguita, le dichiarazioni rese dal soggetto così individuato. In un or-

⁴L'inciso relativo alla cancellazione non figurava nella versione del 10 giugno ed è stato inserito in sede di trasmissione alle Camere. Analogamente, il co. 1 è stato integrato con il requisito, non previsto in origine, della reclusione non inferiore nel massimo a quattro anni.

dinamento che, com'è noto, non conosce una regola generale di invalidità derivata in materia probatoria e nel quale la giurisprudenza di legittimità mantiene sul punto un orientamento restrittivo⁵, la delimitazione non è neutra: il *match* biometrico esce dal fascicolo, mentre vi permane tutto ciò che esso ha generato. Ma di questo profilo – che meriterebbe autonomo sviluppo – qui non si discute. Si discute della condizione, logicamente anteriore, perché la sanzione possa essere anche solo invocata.

3. *Il presupposto tacito dell'inutilizzabilità: la notizia dell'atto.* Ogni divieto probatorio postula, sul piano operativo, un antecedente di fatto: che la parte interessata sappia che l'atto vietato è stato compiuto. È un presupposto talmente ovvio da restare, di regola, implicito, e appunto per questo il codice non lo enuncia: lo realizza, disponendo per ciascun atto a formazione unilaterale un corrispondente meccanismo di *discovery*. La rilevabilità d'ufficio non muta i termini del problema, poiché anche il giudice può rilevare soltanto ciò di cui gli atti danno conto.

Conviene precisare in quale senso la conoscibilità rilevi, giacché il punto è esposto a un equivoco. Non si assume che essa costituisca elemento strutturale dell'inutilizzabilità: l'art. 191 c.p.p. opera oggettivamente e il divieto di utilizzazione consegue alla violazione del divieto di acquisizione a prescindere dallo stato di conoscenza delle parti. Occorre però tenere distinti quattro piani, che il discorso corrente tende a sovrapporre: l'esistenza della sanzione, che dipende dalla previsione legale; la sua rilevabilità, che dipende dal regime processuale del vizio; la conoscibilità del fatto che la genera, che dipende dalla disciplina documentale e ostensiva dell'atto; l'effettività del rimedio, che dalla conoscibilità dipende per intero. Fra il primo piano e il quarto corre la distanza che separa un divieto vigente da un divieto azionabile. La tesi qui sostenuta si colloca sul terzo piano e riguarda dunque non la struttura dell'invalidità, ma la condizione processuale della sua effettività: l'ordinamento può ben comminare una sanzione probatoria senza che alcuno ne conosca il presupposto e la sanzione resterà giuridicamente esistente; ciò che verrà meno è la sua attitudine a operare, la quale è poi la sola ragione per cui essa è stata prevista.

⁵Sul tema, cfr., GALANTINI, *Alla ricerca della «inutilizzabilità derivata»*, in *Sistema penale*, 24 marzo 2021, e ID., L'art. 191 c.p.p. a confronto con la «inutilizzabilità derivata» in un nuovo giudizio costituzionale, ivi, 18 gennaio 2022.

L'eccezione di inutilizzabilità ex art. 359-ter, co. 8 presuppone dunque che la difesa sia in grado di stabilire, quanto meno: che il sistema è stato impiegato; in quale arco temporale e in quale area geografica; sulla scorta di quale provvedimento; con quale banca dati di riferimento; e – ove si intenda contestare non la legalità formale dell'impiego ma l'attendibilità dell'esito – con quale sistema, con quale soglia operativa e con quale tasso di errore rilevato. Sono, questi ultimi, i dati che assegnano al risultato biometrico la sua reale portata dimostrativa: un confronto automatizzato non produce un'identificazione, ma un grado di somiglianza al quale l'operatore attribuisce, o nega, valore identificativo in base a una soglia predeterminata.

I dati così elencati non assolvono, peraltro, la medesima funzione, e la distinzione merita di essere tenuta ferma. I primi – l'avvenuto impiego, le coordinate temporali e spaziali, il provvedimento abilitante, la banca dati interrogata – servono a controllare la legalità dell'atto, cioè a verificare se ricorressero i casi consentiti e se siano state osservate le condizioni dei commi 6 e 7: costituiscono, in altri termini, il presupposto conoscitivo della deduzione ex co. 8. I secondi – il sistema, la soglia operativa, il tasso di errore – servono a discutere l'attendibilità del risultato, e attengono alla valutazione della prova più che alla sua ammissibilità. Solo per i primi si pone un problema di conoscibilità necessaria e tipizzata; per i secondi la questione è di accesso graduato, componibile con le esigenze di riservatezza industriale. Non si postula, dunque, un diritto della difesa a ripercorrere il funzionamento dell'algoritmo, che convertirebbe il processo penale in una verifica tecnica sui sistemi; si postula il diritto a conoscere quanto è necessario a rendere contestabile l'atto che ha inciso sulla propria posizione processuale.

Nessuno di questi elementi forma oggetto, nella disciplina in esame, di un obbligo di documentazione, di deposito o di ostensione alla parte. Non occorre spingersi ad affermare che la difesa non ne verrà mai a conoscenza – la prassi conosce vie oblique, e l'assunto non sarebbe comunque dimostrabile in astratto: è sufficiente, ed è assai più grave, constatare che l'ordinamento non lo assicura, non disciplinando né i tempi, né i contenuti, né le forme di quella conoscenza. Vi si aggiunga un riflesso ulteriore, che il difetto di conoscibilità produce sul terreno della derivazione: se la matrice biometrica dell'indagine resta ignota, non è soltanto il *match* a sottrarsi al controllo, ma la possibilità stessa di interrogarsi sulla genealogia degli atti che ne sono seguiti.

4. *Ciò che la disciplina produce, e a chi è destinato.* Non si sostiene che il decreto trascuri la tracciabilità. Al contrario, l'art. 9 – espressamente riferito tanto all'art. 8 quanto all'art. 359-ter c.p.p. – costruisce un apparato articolato: valutazione d'impatto preventiva sui diritti fondamentali ai sensi dell'art. 27 del regolamento; registrazione automatica di ogni utilizzo in *file* di *log* non modificabili, comprendenti i dati previsti dall'art. 12, par. 3, del medesimo regolamento, conservati per cinque anni; notifica al Garante successiva all'utilizzo; e rinvio a un decreto ministeriale per l'individuazione dei requisiti tecnici minimi di affidabilità e accuratezza, delle modalità di monitoraggio dei *bias* e delle informazioni che il titolare del trattamento è tenuto ad allegare alla richiesta di autorizzazione, in ordine alle caratteristiche tecniche del sistema, ai risultati delle verifiche di accuratezza e ai meccanismi di gestione degli errori. L'apparato esiste. È la sua destinazione a essere significativa. I *file* di *log* sono resi accessibili, recita il co. 2, «esclusivamente alle sole autorità competenti» per finalità di verifica della liceità del trattamento, di controllo interno e nell'ambito di un procedimento penale: formula che individua i destinatari per qualifica pubblicistica e non contempla la parte privata. Le informazioni tecniche di cui al co. 5, lett. *f* sono allegate alla *richiesta* di autorizzazione, e circolano dunque nella sequenza – unilaterale e coperta da segreto investigativo – che va dalla polizia giudiziaria al pubblico ministero e da questi al giudice. Non è previsto che raggiungano, in alcun momento e con alcuna forma, il difensore. La valutazione d'impatto è adempimento del titolare del trattamento. La notifica ha come destinatario il Garante ed è differibile per esigenze di segretezza fino a sei mesi.

Manca, correlativamente, ogni previsione dal versante processuale: non un obbligo di dare atto dell'impiego nel fascicolo delle indagini; non un termine di deposito del decreto autorizzativo e dell'eventuale provvedimento di convalida; non una documentazione tipica delle operazioni; non un'indicazione, nel decreto del giudice per le indagini preliminari, del sistema utilizzato e della banca dati di riferimento, che il co. 6 non annovera fra i contenuti necessari del provvedimento⁶.

⁶ La lacuna non è imputabile a disattenzione del legislatore delegato verso i rilievi formulati in sede consultiva. Il testo definitivo ha infatti recepito le condizioni poste dal Garante per la protezione dei dati personali, integrando il co. 3 con la prescrizione che la banca dati di riferimento sia formata appositamente per ciascun utilizzo, con i soli dati biometrici pertinenti alla specifica finalità, cancellati al termine della validità dell'autorizzazione e non suscettibili di alimentazione incrementale, e con il divieto espresso di impiegare banche dati alimentate mediante tecniche di *scraping* non mirato. Il confronto fra le

Un ulteriore elemento merita segnalazione e riguarda proprio la soglia operativa. La versione dello schema licenziata dal Consiglio dei ministri il 10 giugno 2026 demandava al decreto ministeriale l'individuazione dei requisiti tecnici minimi di affidabilità e accuratezza «ivi incluse le soglie operative utilizzabili». L'inciso è stato soppresso nel testo trasmesso alle Camere. Il parametro dal quale dipende, più di ogni altro, il rapporto fra falsi positivi e falsi negativi è così uscito dal contenuto obbligatorio della fonte secondaria; e la fonte secondaria non è assistita da alcun termine di adozione: il testo definitivo ha anzi soppresso il termine di tre mesi che l'atto n. 418 prevedeva per l'omologo decreto ministeriale in materia di riconoscimento facciale a posteriori, oggi contemplato dall'art. 10, co. 12 sicché l'intero apparato tecnico di garanzia resta affidato a fonti di cui non è scandita l'adozione.

5. *Una controprova interna al decreto.* Si potrebbe obiettare che l'assenza di strumenti conoscitivi rifletta un'oggettiva difficoltà: la documentazione tecnica dei sistemi è coperta da segreti commerciali, il funzionamento degli algoritmi è opaco, la *disclosure* integrale sarebbe incompatibile con le esigenze investigative. L'obiezione è seria, e sarebbe decisiva se il legislatore delegato non avesse già dimostrato, nel medesimo testo, di saperla superare.

Il Capo II del Titolo II del decreto disciplina infatti gli strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale. L'art. 17 attribuisce al giudice il potere di ordinare, su istanza di chi allega di avere subito il danno, l'esibizione degli elementi di prova specificamente pertinenti relativi al funzionamento del sistema; e individua espressamente, fra tali elementi, i registri di cui all'art. 12 del regolamento, la documentazione relativa al sistema di gestione dei rischi di cui all'art. 9, le informazioni contenute nella documentazione tecnica di cui all'art. 11 e le informazioni relative ai parametri e alle modalità di supervisione umana di cui all'art. 14. Lo *standard* di accesso è quello, deliberatamente tenue, della verosimiglianza. Il rischio di divulgazione di segreti commerciali non preclude l'ordine, ma ne condiziona le modalità, mediante rinvio all'art. 121-ter del codice della proprietà industriale. E l'inadempimento è presidiato: il giudice può desumere argomenti di prova ex art. 116 c.p.c. e, quando

due versioni è dunque istruttivo: là dove un'autorità si è pronunciata, la fattispecie è stata emendata; il versante delle prerogative difensive, sul quale nessun organo consultivo si è espresso, è rimasto immutato.

l'inadempimento riguardi la documentazione tipizzata, ritiene come ammessi i fatti allegati dall'istante.

Il confronto non ha valore retorico. Esso dimostra tre cose. La prima è che l'accesso alla documentazione tecnica di un sistema di intelligenza artificiale è tecnicamente praticabile: lo stesso legislatore lo ha costruito. La seconda è che l'esigenza di riservatezza industriale non costituisce ostacolo insuperabile, ma un interesse componibile mediante cautele procedurali. La terza è che l'ordinamento sa individuare con precisione, per rinvio agli obblighi documentali già imposti dal regolamento, l'oggetto dell'ostensione: gli artt. 9, 11, 12 e 14 del regolamento IA sono richiamati uno per uno.

Ne discende un esito che merita di essere enunciato senza attenuazioni. Nel medesimo provvedimento normativo, chi lamenta un pregiudizio patrimoniale derivante dal funzionamento di un sistema di intelligenza artificiale dispone di uno strumento tipizzato, presidiato e azionabile per accedere agli elementi che ne documentano il funzionamento; chi subisce l'impiego del medesimo sistema quale strumento di identificazione o di localizzazione nell'ambito di un procedimento penale non dispone di alcuno strumento corrispondente, e neppure della notizia che gli consentirebbe di invocarlo. La gerarchia dei beni è rovesciata: la garanzia è più intensa dove l'interesse in gioco è patrimoniale, e recede dove sono in gioco la libertà personale e il diritto di difesa.

6. Il raffronto con i modelli codicistici, con la disciplina parallela e con le esperienze straniere. Il rilievo si precisa ulteriormente ove si consideri che il codice, per ogni atto a formazione unilaterale assistito da sanzione probatoria, predispone la corrispondente sequenza conoscitiva.

Il paradigma delle intercettazioni – al quale la relazione illustrativa dichiara di ispirarsi quanto al meccanismo dell'urgenza, richiamando l'art. 267, co. 2 – non si esaurisce nel procedimento autorizzativo. Esso comprende l'archivio di cui all'art. 269, il deposito dei verbali e delle registrazioni, la facoltà dei difensori di esaminare gli atti e ascoltare le registrazioni, la procedura di stralcio, il regime di distruzione. È quella seconda metà a rendere effettiva l'inutilizzabilità dell'art. 271. Del paradigma, l'art. 359-ter recepisce la prima metà e omette la seconda.

Analoga considerazione vale per gli atti collocati nella medesima sede codicistica. L'art. 360 c.p.p. subordina l'accertamento tecnico non ripetibile all'avviso al difensore, con facoltà di assistervi e di nominare consulenti; l'art.

359-*bis* c.p.p., immediatamente precedente alla disposizione in commento, dispone che del decreto e delle operazioni da compiersi sia data tempestivamente notizia al difensore dell'interessato, che ha facoltà di assistervi, con richiamo ai commi 1 e 2 dell'art. 365 c.p.p., e stabilisce che l'avviso della decisione di convalida sia dato immediatamente anche al difensore; il co. 3 sanziona poi con la nullità delle operazioni e l'inutilizzabilità delle informazioni acquisite la violazione delle disposizioni ivi richiamate, dichiarando espressamente applicabile l'art. 191, co. 2 c.p.p. La disposizione immediatamente precedente a quella in esame accoppia dunque, in un unico articolo, la sanzione probatoria e il meccanismo che ne consente la deduzione. La collocazione dell'art. 359-*ter* nel Titolo V del Libro V, fra le attività del pubblico ministero, risulta così doppiamente problematica: sul piano della qualificazione dell'atto, come già rilevato in dottrina; e sul piano della coerenza interna, perché la disposizione si sottrae al regime partecipativo che caratterizza gli atti fra i quali è stata inserita⁷.

Un ulteriore riscontro si trae dall'interno del medesimo decreto e precisamente dalla disciplina che il testo definitivo ha riservato al riconoscimento facciale a posteriori. L'art. 10, co. 2 subordina l'impiego delle tecnologie di riconoscimento integrate nei sistemi di videosorveglianza, quando esse siano dirette alla ricerca mirata di una persona indiziata della commissione di un reato, a un'autorizzazione del giudice per le indagini preliminari: il pubblico ministero, su istanza degli ufficiali di polizia giudiziaria che hanno avviato i sistemi, la richiede senza ritardo e comunque entro quarantotto ore dall'avvio, e il giudice provvede con decreto motivato nelle successive quarantotto ore. L'inosservanza dei termini, o il diniego, comportano l'immediata interruzione dell'impiego e la cancellazione di tutti i dati personali, dei risultati e degli *output* acquisiti e prodotti, salvo che costituiscano corpo del reato; mentre il comma 3, per l'ipotesi residua dell'identificazione iniziale compiuta sulla base di elementi oggettivi e verificabili direttamente connessi al fatto di reato, commina espressamente l'inutilizzabilità dei risultati. Si tratta di previsioni che

⁷Va peraltro osservato che la relazione illustrativa individua la sede nel «Titolo IV del Libro V», mentre le attività del pubblico ministero sono disciplinate dal Titolo V; e che la medesima relazione afferma che la collocazione «riflette la natura dello strumento quale mezzo di ricerca della prova nelle indagini preliminari», quando i mezzi di ricerca della prova sono raccolti nel Titolo III del Libro III. L'argomento, così formulato, si autoconfuta.

l'atto del Governo n. 418 non contemplava, e che segnano un irrobustimento del controllo giurisdizionale rispetto allo schema.

Il dato merita attenzione proprio perché rivela la direzione dell'intervento correttivo. Nel passaggio dallo schema al testo definitivo il legislatore delegato ha esteso la riserva di giurisdizione a un'attività che ne era priva, ne ha scandito i tempi e ha articolato le conseguenze della loro inosservanza. Nulla, per contro, ha disposto quanto alla documentazione dell'operazione, al deposito del provvedimento autorizzativo e alla conoscibilità dell'impiego da parte della difesa. L'asse dell'intervento è rimasto quello del controllo del giudice sull'autorità procedente; quello del controllo della parte sull'atto compiuto non è stato sfiorato. Ciò che si è inteso rafforzare, in entrambe le sedi, è il momento genetico dell'attività: il momento ostensivo è rimasto estraneo alla prospettiva del legislatore delegato.

Vi è infine un termine di paragone esterno, di data pressoché coeva, che rende evidente il carattere di scelta dell'omissione. Il 10 luglio 2026 il Bundestag ha approvato, nel testo licenziato dalla Commissione interni, la riforma della legge sulla polizia federale, che introduce un § 31b dedicato alla «rilevazione biometrica in tempo reale». Vi si rinvencono, accanto alla riserva di giurisdizione e alla rigorosa delimitazione temporale del provvedimento, quattro previsioni che qui interessano: la corrispondenza automaticamente proposta dal sistema deve essere verificata, prima di ogni ulteriore trattamento, da due agenti separatamente e appositamente formati sui rischi dell'impiego dell'intelligenza artificiale; l'istanza rivolta al giudice e il provvedimento che l'accoglie devono indicare il produttore e la denominazione commerciale del sistema impiegato; la verbalizzazione della misura deve dare conto della persona presa di mira e del numero delle corrispondenze falsamente positive; la persona interessata, infine, deve essere successivamente informata dell'applicazione della misura, a tal fine inserita nel catalogo degli atti soggetti a obbligo di notizia⁸.

⁸Entwurf eines Gesetzes zur Modernisierung des Bundespolizeigesetzes, BT-Drs. 21/3051 del 3 dicembre 2025; Beschlussempfehlung und Bericht des Innenausschusses, BT-Drs. 21/6990 dell'8 luglio 2026, che, accogliendo l'emendamento delle frazioni CDU/CSU e SPD (Ausschussdrucksache 21(4)192), inserisce nel testo i §§ 31a e 31b BPolG-E. Le previsioni richiamate sono, rispettivamente, il § 31b, Abs. 2, Satz 1 e 5 (verifica separata da parte di due agenti formati sui rischi dell'intelligenza artificiale, con divieto di conservazione dei dati acquisiti ove il riscontro risulti negativo), il § 31b, Abs. 4, Nr. 6, e Abs. 5, Nr. 5 (indicazione del produttore e della denominazione del prodotto tanto nell'istanza quanto nel provvedimento del giudice, il quale non può eccedere le settantadue ore), il § 85, Abs. 2, Nr. 3 (verba-

Il raffronto va condotto con cautela, giacché la disposizione tedesca appartiene al diritto di polizia e opera sul terreno della prevenzione, dove manca per definizione una parte processuale cui rendere conto. Proprio per questo, tuttavia, l'argomento si rafforza anziché indebolirsi: se il presidio conoscitivo – verifica umana documentata, tracciamento dei falsi positivi, identificazione del sistema negli atti autorizzativi, avviso successivo all'interessato – è parso necessario là dove nessun procedimento è in corso, difficilmente potrà dirsi superfluo là dove l'atto è destinato a produrre effetti nel processo penale. Il legislatore italiano poteva conoscere, e non ha adottato, un modello che rende il risultato biometrico verificabile senza pregiudizio per l'efficacia dell'indagine.

Un secondo termine di raffronto, questa volta giurisprudenziale, conferma che la questione non è un artificio dottrinale. Il 24 giugno 2026 la Corte suprema del New Jersey, pronunciandosi su una richiesta di *discovery* relativa a un'identificazione ottenuta mediante riconoscimento facciale, ha stabilito che l'accusa deve comunque rendere note l'identità degli strumenti impiegati e le modalità del loro impiego nell'indagine – e ciò anche quando non intenda avvalersi in giudizio del risultato del confronto –, riservando invece a una verifica caso per caso, subordinata alla dimostrazione di un bisogno specifico, l'accesso alle informazioni coperte da segreto industriale, quale il codice sorgente⁹. La decisione è, per il tema qui trattato, doppiamente istruttiva. Sul piano del contenuto, perché individua esattamente la soglia minima che si va sostenendo: sapere che il sistema è stato impiegato e come, prima e indipendentemente dal sapere come esso funzioni. Sul piano del metodo, perché quel risultato è stato raggiunto in via giurisprudenziale, entro un ordinamento che affida la *discovery* a regole generali ed elastiche, presidiate da un obbligo costituzionale di ostensione. Nel nostro, dove la circolazione degli atti

lizzazione della persona presa di mira e del numero dei falsi positivi) e il § 78, Abs. 1, Nr. 3 (obbligo di informazione della persona interessata); vi si aggiungono l'estensione al § 31b dei poteri del Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (§ 77) e l'obbligo di valutazione su base scientifica a due anni dall'attivazione del sistema (§ 106, Abs. 3). Il testo è stato approvato dal Bundestag in seconda lettura il 10 luglio 2026 e, alla data in cui si scrive, attende l'esame del Bundesrat. ⁹Supreme Court of New Jersey, 24 giugno 2026, *State v. Miles* (A-41-24), che supera la meccanica applicazione dell'elenco di tredici categorie di elementi ostensibili enucleato da *State v. Arteaga* (App. Div., 2023), affermando la necessità di modulare l'ostensione in relazione alle circostanze del caso, ma confermando l'obbligo di rendere note le tecnologie impiegate e le modalità del loro impiego a fini identificativi e investigativi. Il dibattito che ha preceduto la pronuncia è ricostruito da Barranco, *Match Up*, cit.

d'indagine è scandita da termini e da sequenze tipiche, e dove il giudice non dispone del potere di istituire un onere di deposito che la legge non contempla, l'omissione non è colmabile in via interpretativa: è, per ciò stesso, destinata a durare quanto dura la lacuna.

7. Il piano della delega e quello convenzionale. Le considerazioni svolte assumono rilievo anche sul terreno della conformità alla legge di delegazione. L'art. 24, co. 5, lett. e) della L. 23 settembre 2025, n. 132 delega il Governo a regolare l'utilizzo dei sistemi di intelligenza artificiale nelle indagini preliminari «nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza». Dei cinque criteri, tre trovano attuazione nell'art. 359-ter: la proporzionalità, mediante la delimitazione soggettiva, spaziale e temporale e il rinvio alle valutazioni di cui all'art. 5, par. 2 del regolamento; la non discriminazione, per il tramite del monitoraggio dei *bias* demandato al decreto ministeriale; la trasparenza, sia pure nella sola dimensione della tracciabilità interna. I due restanti – il diritto di difesa e i dati personali dei terzi – non ricevono alcuna disposizione attuativa.

La circostanza è, del resto, indirettamente confermata dallo stesso Governo: l'analisi di impatto della regolamentazione, nell'enunciare gli obiettivi specifici perseguiti, indica il tracciamento di un perimetro di liceità «con riserva di giurisdizione, limiti temporali rigorosi e sanzione di inutilizzabilità», senza menzione alcuna del diritto di difesa né della posizione dei terzi. Sembra dunque configurabile, sul punto, un vizio di eccesso di delega ai sensi dell'art. 76 Cost., nella forma dell'attuazione parziale del criterio direttivo.

Si obietterà che il criterio, per la sua ampiezza, lascia al delegato un margine di apprezzamento e che il rispetto delle garanzie difensive avrebbe potuto essere assicurato secondo modalità diverse da quelle qui prospettate. L'obiezione coglierebbe nel segno se si contestasse la scelta fra tecniche alternative – il deposito anziché l'avviso, l'accesso su istanza anziché l'ostensione automatica –, giacché la selezione dei mezzi appartiene senza dubbio al delegato. Ciò che si rileva è altro: che nessuna delle tecniche possibili è stata adottata, sicché il criterio non risulta attuato in misura minore, ma non risulta attuato affatto; e la differenza fra il meno e il nulla è, in materia di delega, la differenza fra l'esercizio e l'omissione del potere conferito. Né varrebbe replicare che il diritto di difesa sia stato presidiato proprio dall'inutilizzabilità del co.

8: l'argomento è circolare, poiché assume come attuazione della garanzia ciò la cui azionabilità dipende dalla garanzia mancante. Resta semmai da stabilire se il vizio debba essere fatto valere *sub specie* di eccesso di delega ovvero se, data l'ampiezza del criterio delegante, non sia più piano il percorso che muove direttamente dagli artt. 24, co. 2 e 111, co. 3 Cost.: la seconda via ha il pregio di non dipendere dal grado di specificità della norma di delegazione, e conduce al medesimo esito, poiché una garanzia difensiva il cui presupposto conoscitivo resti nella disponibilità esclusiva della parte pubblica non è, in senso proprio, una garanzia.

Sul versante convenzionale, la Corte europea dei diritti dell'uomo ha affermato, in tema di tecnologie di riconoscimento facciale, la necessità di regole dettagliate che ne governino ambito e applicazione, nonché di solide garanzie contro il rischio di abuso e arbitrarietà¹⁰. Una garanzia contro l'arbitrarietà è solida nella misura in cui è azionabile da chi ne è destinatario, secondo il canone – costante nella giurisprudenza convenzionale – per cui i diritti devono essere concreti ed effettivi, non teorici e illusori; una garanzia il cui presupposto conoscitivo resti nella disponibilità esclusiva dell'autorità procedente ne condivide il nome, non la funzione. Vi si aggiunga che il considerando 73 del regolamento richiede, per i sistemi di identificazione biometrica, che nessuna azione o decisione sia adottata sulla base dell'identificazione senza verifica e conferma separata da parte di almeno due persone fisiche: requisito che lo schema non recepisce¹¹ e la cui assenza si riverbera sul tema qui trattato, poiché sottrae al fascicolo la traccia documentale di una verifica che non è imposta.

8. *Ipotesi ricostruttive*. Se la diagnosi è esatta, la terapia non richiede un ripensamento dell'istituto, ma l'innesto di una sequenza conoscitiva che ne renda azionabile la sanzione. Se ne indicano gli elementi minimi.

(a) Documentazione dell'operazione. Andrebbe previsto che delle operazioni sia redatto verbale, da inserire nel fascicolo del pubblico ministero, recante

¹⁰Corte EDU, 4 luglio 2023, Glukhin c. Russia, spec. §§ 75, 82 e 87. Sui riflessi della pronuncia sull'ordinamento interno, GIALUZ, *Riconoscimento biometrico*, cit.

¹¹Sul punto v. Sacchetto, *Tecnologie di riconoscimento facciale e procedimento penale*, Giappichelli, 2025, p. 193, che valorizza la funzione del doppio controllo rispetto ai *bias* algoritmici e ai condizionamenti cognitivi dell'operatore; DELLA TORRE, *Quale spazio per gli strumenti di riconoscimento facciale nella giustizia penale?*, in *Intelligenza artificiale e processo penale. Indagini, prove, giudizio*, a cura di Di Paolo-Pressacco, Napoli, 2022, p. 7 ss.

l'indicazione del provvedimento autorizzativo, dell'arco temporale e dell'area interessata, della banca dati di riferimento e dell'esito, positivo o negativo, del confronto. La verbalizzazione dei *non-match* non è dettaglio pedantesco: il numero dei confronti negativi è elemento essenziale per apprezzare l'affidabilità di quello positivo.

(b) Deposito, termine e avviso. Il decreto autorizzativo, l'eventuale provvedimento di convalida e il verbale dovrebbero essere depositati, con facoltà di ritardo motivato per esigenze investigative e comunque non oltre la chiusura delle indagini preliminari, in coerenza con la funzione di *discovery* assolta dall'art. 415-*bis* c.p.p. Al soggetto identificato che non assuma la qualità di indagato – ipotesi tutt'altro che marginale, trattandosi di strumento che opera su una pluralità indeterminata di volti – il deposito nulla garantisce: per costui occorrerebbe un avviso successivo, sul modello ora accolto dal legislatore tedesco, differibile e in casi determinati omissibile, ma non pretermissibile in linea di principio.

(c) Accessibilità difensiva della documentazione tecnica. Il difensore dovrebbe poter accedere ai *file* di *log* di cui all'art. 9, co. 2 e alle informazioni tecniche allegate alla richiesta ai sensi del co. 5, lett. *f*) con le cautele previste per la tutela dei segreti commerciali. Il modello è disponibile e si trova, come si è visto, nell'art. 17 del medesimo decreto.

(d) Reintegrazione della soglia operativa. Il riferimento alle soglie operative utilizzabili, soppresso in corso di *iter*, andrebbe restituito al contenuto obbligatorio del decreto ministeriale, che dovrebbe inoltre essere corredato di un termine di adozione.

(e) Verifica umana rafforzata. Andrebbe recepito il requisito della conferma separata da parte di due operatori, con documentazione della verifica.

(f) Regime della distruzione e divieto di utilizzo indiretto. La cancellazione prevista dal co. 8 dovrebbe essere assistita da un procedimento in contraddittorio sul modello dell'art. 269, co. 2 c.p.p. e accompagnata da una previsione espressa che estenda il divieto di utilizzo agli elementi direttamente derivati dal risultato inutilizzabile. In difetto, la sanzione conserva un'efficacia meramente nominale.

9. *Rilievo conclusivo*. Il nuovo art. 359-*ter* c.p.p. non difetta di garanzie: ne dispone parecchie, e alcune non banali. Difetta del meccanismo che le rende esigibili. La riserva di giurisdizione presidia il momento genetico dell'atto;

l'inutilizzabilità ne presidia, in astratto, il momento patologico; ma fra i due momenti non è collocato ciò che consente alla parte di avvedersi che la patologia si è verificata. Ne risulta un divieto probatorio ammesso in astratto e precluso in concreto, poiché l'onere di allegazione grava su chi non dispone dell'atto da censurare.

Non si tratta, si ribadisce, di un difetto di intensità della tutela, rispetto al quale si potrebbe discutere di opportunità e di bilanciamenti. Si tratta di un vizio di costruzione della fattispecie: la norma commina una sanzione e non predispone la condizione della sua applicazione. La circostanza che il medesimo decreto legislativo abbia predisposto quella condizione, in termini analitici, a beneficio dell'attore in un giudizio risarcitorio, priva l'omissione di ogni giustificazione tecnica. Ne discende, per necessità, la sua qualificazione come scelta; e poiché la scelta consiste nel non predisporre la condizione di esercizio di una garanzia che la Costituzione impone di assicurare a chi è sottoposto al procedimento, e che la legge di delegazione imponeva espressamente di rispettare, essa non appartiene all'area del merito legislativo insindacabile, ma a quella della conformità agli artt. 24, co. 2 e 111, co. 3 Cost., nonché all'art. 76 Cost. Al legislatore delegato non si chiede di aver scelto bene fra più soluzioni possibili: gli si chiede di averne scelta una.