



DAVIDE TUTINO

Intelligenza artificiale e responsabilità

Il decreto legislativo
9 settembre 2026, n. 160

AVVOCATO PENALISTA DEL FORO DI CATANIA

Dottore di ricerca, Università degli Studi di Catania

SETTEMBRE 2026

Intelligenza artificiale e responsabilità

Il decreto legislativo 9 settembre 2026, n. 160

di Davide TUTINO

SOMMARIO: 1. La misura della decisione. — 2. Prima e dopo il decreto: la trama delle fonti. — 3. La geografia dei soggetti e dei dati. — 4. Dalla ricerca all'impiego: il controllo umano. — 5. Il volto e la prevenzione: identificazione biometrica in tempo reale. — 6. La ricerca nel procedimento penale. — 7. Il riconoscimento facciale a posteriori. — 8. Pericolo, colpevolezza e responsabilità dell'ente. — 9. Il danno, la prova e la presunzione causale. — 10. Assicurazione, tempo della legge e responsabilità della decisione.

1. La misura della decisione

Il decreto legislativo 9 settembre 2026, n. 160, interviene in un ambito nel quale la possibilità tecnica di ottenere un risultato non coincide con il potere di farne uso. Una corrispondenza fra immagini può indicare una persona da cercare, senza accertarne da sola l'identità; una classificazione di rischio può orientare l'attività di polizia, senza sostituire la decisione dell'autorità competente. Per comprendere come il decreto governi questo passaggio occorre partire dalle fonti europee e dalla delega nazionale, quindi seguire il sistema nella ricerca, nella sperimentazione e nell'attività delle Forze di polizia. La disciplina dell'identificazione biometrica consentirà di osservare come mutino presupposti, autorità e sorte del risultato quando dalla prevenzione si passa al procedimento penale, e come la ricerca successiva all'acquisizione delle immagini si distingua da quella in tempo reale. Saranno poi esaminate le condotte che espongono a pericolo la vita, l'incolumità o la sicurezza dello Stato e, sul diverso piano della tutela civile, le regole che permettono al danneggiato di accedere alla prova e a un'eventuale copertura assicurativa. In ciascun ambito il problema della responsabilità assume una forma propria: riguarda la legittimità dell'operazione, l'attribuzione di una condotta penalmente rilevante oppure l'accertamento del danno e del suo nesso con la violazione di un obbligo. È attraverso queste diverse forme, e non mediante una categoria indifferenziata di «decisione algoritmica», che si può valutare la portata del decreto.

2. Prima e dopo il decreto: la trama delle fonti

Prima del decreto, l'impiego dell'intelligenza artificiale non era lasciato a una libertà indifferenziata. Il regolamento (UE) 2024/1689 aveva già ordinato le pratiche e i sistemi in relazione ai rischi; la direttiva (UE) 2016/680, attuata dal d.lgs. 18 maggio 2018, n. 51, regolava i dati personali trattati dalle autorità competenti per finalità di polizia. La legge 23 settembre 2025, n. 132, ha quindi affidato al Governo un compito più circoscritto di quanto suggerisca l'idea di una disciplina nazionale «dell'IA»: l'art. 24, comma 2, lett. h), riguarda la polizia, mentre i commi 3 e 5 investono i presidi penali e processuali e la tutela risarcitoria. Il d.lgs. n. 160 del 2026 si colloca all'incrocio di questi percorsi. Per gli impieghi di polizia, la fonte europea delimita ciò che può essere consentito; quella nazionale stabilisce, entro quel limite, chi possa agire e in quale forma.¹

Il regolamento europeo vieta alcune pratiche, classifica taluni sistemi come ad alto rischio e collega alla classificazione obblighi differenziati. Per l'identificazione biometrica remota in tempo reale negli spazi accessibili al pubblico a fini di contrasto dei reati, l'art. 5, par. 1, primo comma, lett. h), formula un divieto accompagnato da eccezioni tassativamente individuate. Il divieto non si trasforma in una generale abilitazione per il solo fatto che un'autorità pubblica persegua un fine di sicurezza. Lo Stato membro può autorizzare, entro i limiti europei, alcuni usi e deve disciplinare la richiesta, la decisione, il controllo e la rendicontazione delle singole autorizzazioni. Il riconoscimento biometrico a posteriori appartiene, invece, a una disciplina diversa: la distinzione dipende dal tempo che separa acquisizione, confronto e identificazione e dalla concreta funzione dell'operazione, non dal nome commerciale del programma.²

Questo rapporto si vede già nei rinvii degli artt. 8 e 359-ter c.p.p. all'art. 5 del regolamento. L'ordinamento interno organizza la richiesta e il controllo delle ricerche biometriche, ma l'eccezione al divieto europeo non può essere ampliata attraverso una formula nazionale più generica. È il primo esempio di una caratteristica che ricorrerà nel capitolo: l'appartenenza di un sistema a una classe di rischio non autorizza il suo impiego da parte della polizia; l'autorizzazione di una singola operazione, a sua volta, non sana un difetto dei dati o del sistema. Le regole sul prodotto e quelle sull'esercizio del potere si incontrano nel medesimo fatto senza perdere la propria autonomia.

1 D.lgs. 9 settembre 2026, n. 160, in *G.U.*, serie generale, 15 settembre 2026, n. 214: testo online. L. 23 settembre 2025, n. 132, art. 24, commi 1, 2, lett. h), 3 e 5: testo online. Reg. (UE) 2024/1689, versione consolidata: testo online. Testo nazionale esaminato al 26 settembre 2026; la pubblicazione ufficiale indica l'entrata in vigore al 30 settembre 2026.

2 Reg. (UE) 2024/1689, artt. 3, punti 41)-43), 5, parr. 1-5, e 26, par. 10. Il portale istituzionale della Commissione rende consultabili le disposizioni, segnalando che alcune pagine riproducono ancora il testo anteriore al regolamento del 2026: testo online; testo online.

Anche il tempo della legge richiede attenzione. Il d.lgs. n. 160 del 2026 è stato pubblicato nella Gazzetta Ufficiale del 15 settembre 2026, n. 214, ed entrerà in vigore il 30 settembre. Nel frattempo, il quadro europeo è stato modificato dal regolamento (UE) 2026/1744, entrato in vigore il 27 luglio 2026. Secondo le informazioni istituzionali della Commissione, gli obblighi del regime dei sistemi ad alto rischio compresi nell'allegato III si applicheranno, in linea generale, dal 2 dicembre 2027; per i sistemi incorporati nei prodotti dell'allegato I il termine è il 2 agosto 2028. L'operatività, già precedente, delle pratiche vietate non va confusa con la diversa decorrenza di tali obblighi. È questo il quadro temporale con cui l'art. 21, comma 2, del decreto nazionale chiede di misurarsi quando rinvia ai termini europei.³

Queste date non differiscono automaticamente l'intero decreto italiano. Le disposizioni nazionali individuano autorità, disciplinano autorizzazioni, introducono un reato e regolano la prova civile: per ciascuna occorre verificare se la regola sia direttamente applicabile dal 30 settembre o presupponga un obbligo europeo non ancora operante. Il problema è particolarmente sensibile per l'art. 437-bis c.p., che richiama misure di sicurezza «previste» per sistemi ad alto rischio. Un'omissione penalmente rilevante richiede l'individuazione della misura dovuta nel caso concreto e del momento in cui era esigibile; la sola classificazione del sistema non basta a colmare quel passaggio.

La stessa legge nazionale delimita il proprio campo con due rinvii non sovrapponibili. L'art. 2, comma 1, lett. e), del decreto, riferito al solo titolo I, descrive il sistema ad alto rischio richiamando l'art. 6 del regolamento in combinazione con l'allegato III. L'art. 11, collocato nel titolo II, rinvia invece alle definizioni dell'art. 3 del regolamento, mentre l'espressione «sistemi di intelligenza artificiale ad alto rischio» nell'art. 437-bis c.p. impone un'interpretazione sistematica che tenga conto della classificazione europea nel suo insieme. Estendere automaticamente la definizione speciale del titolo I alla norma penale sarebbe un passaggio da dimostrare, non un dato testuale. Anche le difformità presenti nei rinvii dell'art. 2, comma 1, lett. p) e q), devono essere registrate per ciò che sono, senza sostituire silenziosamente al testo pubblicato una versione ipoteticamente corretta.⁴

Il rilievo costituzionale ed europeo del problema non si esaurisce nella riservatezza, benché il trattamento biometrico incida sulla vita privata e sulla protezione dei dati, tutelate dagli artt. 7 e 8 della Carta dei diritti fondamentali

³ Reg. (UE) 2026/1744, in vigore dal 27 luglio 2026: testo online. Commissione europea, *AI Omnibus enters into force*, 27 luglio 2026, sulle nuove decorrenze: testo online. D.lgs. n. 160 del 2026, art. 21, comma 2.

⁴ Nell'art. 2, comma 1, lett. p) e q), il regolamento è indicato come «(UE) 1689/2024»; la lett. q) rinvia inoltre a una «lettera s)» non presente nell'elenco. La lett. p) è un possibile riferimento sistematico per quest'ultimo rinvio, non una rettifica del testo. Versione pubblicata: testo online.

dell'Unione europea. Una ricerca in uno spazio aperto al pubblico può riflettersi sulla libertà di movimento e sulla partecipazione a riunioni e manifestazioni; gli errori differenziati del sistema interrogano il divieto di discriminazione; la difficoltà di conoscere le condizioni di un'identificazione investe la difesa e il ricorso effettivo. Sul versante penale rilevano la legalità e la presunzione d'innocenza. Nessuna di queste garanzie determina da sola l'esito di ogni operazione. Esse esigono però che la necessità e la proporzionalità siano valutate in concreto, da soggetti individuati e sulla base di dati conoscibili. Per questo, dopo il rapporto fra le fonti, occorre esaminare la distribuzione delle competenze e delle informazioni all'interno del sistema.

3. La geografia dei soggetti e dei dati

Per individuare chi possa servirsi del sistema, il titolo I si rivolge agli organi, uffici e comandi delle Forze di polizia nell'esercizio delle rispettive funzioni; la definizione dell'art. 2, comma 1, lett. o), rinvia all'art. 16 della legge 1° aprile 1981, n. 121. L'appartenenza a una Forza di polizia non basta tuttavia a rendere lecito qualunque impiego della tecnologia. Occorrono una funzione attribuita, una finalità compresa nell'ambito della disciplina e l'osservanza delle condizioni proprie dell'operazione. Quando la legge richiede una autorizzazione per la ricerca biometrica, tale requisito si aggiunge al potere di svolgere l'attività di polizia e ne delimita l'esercizio nel caso concreto.⁵

All'interno di quel perimetro si distribuiscono ruoli ulteriori. AgID e ACN sono le autorità nazionali per l'intelligenza artificiale secondo l'art. 20 della legge n. 132 del 2025; il Garante per la protezione dei dati personali conserva le proprie attribuzioni sul trattamento. Università, enti di ricerca e soggetti pubblici o privati possono collaborare alla ricerca e alla sperimentazione; il Ministero dell'interno, Dipartimento della pubblica sicurezza, è indicato dall'art. 10, comma 5, quale titolare dei trattamenti effettuati attraverso i sistemi ivi disciplinati. Il pubblico ministero, il giudice per le indagini preliminari e, per gli interventi urgenti previsti dalla legge, gli ufficiali di polizia giudiziaria intervengono secondo competenze differenti. Parlare genericamente di «controllo dell'autorità» oscurerebbe proprio la sequenza che rende sindacabile l'uso del sistema.

La pluralità delle autorità non comporta una ripartizione esclusiva delle questioni secondo etichette semplici. Un'autorizzazione del procuratore o del giudice non sostituisce la valutazione d'impatto che spetta al titolare del trattamento; una verifica del Garante non accerta il fatto di reato e non attribuisce

⁵ D.lgs. n. 160 del 2026, artt. 1 e 2; l. 1° aprile 1981, n. 121, art. 16. Per le competenze di AgID e ACN, l. n. 132 del 2025, art. 20.

valore probatorio a un confronto biometrico. Allo stesso modo, il controllo tecnico dell'accuratezza non stabilisce se una ricerca fosse necessaria in quel luogo e per quella persona. Ciascuna competenza illumina un aspetto dell'operazione, e l'ordinamento ne richiede la coesistenza proprio perché nessuna può assorbire le altre. Questa è la ragione istituzionale per cui la documentazione degli accessi, delle autorizzazioni e delle revisioni umane acquista un rilievo che va oltre l'amministrazione interna del sistema.

Il secondo confine riguarda i dati. L'art. 2 distingue categorie particolari di dati personali, dati relativi a condanne e reati e dati operativi sensibili. Questi ultimi non sono semplicemente sinonimo di «dati sensibili»: il riferimento europeo concerne informazioni operative la cui divulgazione potrebbe compromettere l'integrità di attività di prevenzione o di procedimenti penali. Quando le Forze di polizia trattano dati personali per i fini indicati, l'art. 3, comma 6, richiama espressamente il d.lgs. n. 51 del 2018. La disciplina generale del regolamento (UE) 2016/679 resta pertinente per i trattamenti che ricadono nel suo ambito, ma non può essere assunta come unica fonte del trattamento per finalità di polizia. La distinzione delle finalità precede quella delle garanzie applicabili.

Nella ricerca e nella sperimentazione queste distinzioni diventano operative. L'art. 4, comma 1, consente progetti con università, enti di ricerca e soggetti pubblici o privati, anche tramite società in house o a totale partecipazione pubblica controllate dallo Stato, nel rispetto delle regole europee sulla concorrenza e sugli aiuti di Stato. Il comma 2 richiede clausole che escludano la condivisione di dati operativi sensibili e l'acquisizione o utilizzazione, anche indiretta, da parte dei collaboratori dei sistemi e delle risorse addestrati per l'attività di polizia, salva la possibilità di utilizzare dati sintetici o dati reali mascherati o pseudonimizzati. Il comma 3 impone di definire sia la titolarità dei risultati, del software e dei dati di addestramento, sia i ruoli e gli obblighi relativi al trattamento dei dati personali. Assicura, in ogni caso, alle Forze di polizia la titolarità dei modelli addestrati su dati operativi sensibili.

La titolarità dei risultati e il ruolo nel trattamento rispondono a problemi diversi. Possedere il modello addestrato non equivale a decidere le finalità e i mezzi del trattamento dei dati personali. I rapporti di collaborazione devono individuare tali ruoli, documentare le operazioni e disciplinare la sicurezza; su questa base diventa possibile ricostruire quali soggetti abbiano operato sui dati e sulle risorse prodotte. La facoltà di usare dati sintetici non dimostra da sola la qualità del modello, così come la pseudonimizzazione non sottrae automaticamente i dati reali alla disciplina dei dati personali. Si tratta, nel primo caso, di controllare la rappresentatività e la validità del risultato e, nel secondo, di

tutelare gli interessati. L'art. 4 assegna responsabilità nella collaborazione, ma non stabilisce una soglia di accuratezza valida per ogni successivo impiego.

Su questo sfondo si comprende il divieto di alimentare banche dati di riconoscimento facciale mediante scraping non mirato, ripreso dagli artt. 8, comma 3, e 359-ter, comma 3, c.p.p. Un archivio delimitato per una ricerca consente di ricostruire perché un'immagine sia entrata nel confronto; una raccolta indiscriminata recide il legame fra il dato e la finalità che ne giustifica l'uso. Anche il successivo controllo umano dipende da questa storia del dato: un operatore non può valutare seriamente una corrispondenza se ignora la provenienza e la qualità della base sulla quale è stata calcolata. Si passa così dalla titolarità delle risorse alla questione della loro sorveglianza durante il funzionamento del sistema.⁶

4. Dalla ricerca all'impiego: il controllo umano

Il controllo dell'operatore comincia, in realtà, prima che vi sia un risultato da leggere. L'art. 3 segue il sistema dalla ricerca all'utilizzo, passando per sperimentazione, sviluppo, addestramento e convalida. Una categoria scelta durante l'addestramento, oppure un errore non rilevato nella validazione, può indirizzare le risposte future senza essere visibile nell'interfaccia usata dall'agente. L'approccio «antropocentrico, proporzionato e fondato sul rischio» del comma 1 va dunque letto in questa dimensione temporale: non basta riservare formalmente a una persona l'ultima parola se le condizioni della sua scelta sono state fissate altrove e non sono più controllabili.⁷

Il comma 3 assegna a sistemi, modelli e output una funzione strumentale e di supporto. Il comma 4 richiede una revisione umana qualificata dei risultati prima del loro impiego in atti e provvedimenti che incidano sulla sfera giuridica degli interessati; la revisione dev'essere svolta da personale individuato dalle procedure interne e documentata in modo da assicurarne la tracciabilità. Il comma 5 prescrive, per i sistemi ad alto rischio, una sorveglianza umana effettiva conforme all'art. 14 del regolamento europeo e personale dotato delle necessarie competenze. La differenza fra i due commi conta. La revisione del risultato interviene sul singolo output prima del suo impiego; la sorveglianza comprende

6 D.lgs. n. 160 del 2026, artt. 4, 8, comma 3, e 13, che inserisce l'art. 359-ter, comma 3, c.p.p.; Reg. (UE) 2024/1689, art. 5, par. 1, lett. e). Il parere del Garante del 14 luglio 2026 aveva chiesto qualità, cancellazione e non incrementalità delle basi di confronto: testo online.

7 D.lgs. n. 160 del 2026, art. 3, commi 1-7. Sul quadro generale dei principi, l. n. 132 del 2025, art. 3. Per il rapporto tra strumenti algoritmici e autorità giuridica, cfr. REICHMAN A., SARTOR G., «Algorithms and Regulation», in *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge, 2021, pp. 131-181; sulla previsione nell'attività di polizia, GALLI F., «Law Enforcement and Data-Driven Predictions at the National and EU Level», ivi, pp. 111-128.

il funzionamento del sistema e la possibilità di riconoscere limiti, anomalie ed effetti pregiudizievoli nel corso dell'uso. Una firma aggiunta a valle dell'elaborazione non prova, da sola, che entrambe le attività siano state svolte.

Si immagini che il programma segnali una possibile identità sulla base di un'immagine poco nitida. La possibilità di respingere il suggerimento ha valore soltanto se l'operatore conosce la qualità della traccia, la base di confronto e l'incertezza del risultato. Per questo la revisione documentata dovrebbe rendere ricostruibili il risultato esaminato, gli elementi indipendenti impiegati per verificarlo e la ragione del suo recepimento o scarto. Non si tratta di un formulario prescritto dal decreto: è una lettura del requisito di revisione «qualificata» e tracciabile. Un'approvazione automatica, anche se sottoscritta da una persona, non spiegherebbe come la segnalazione sia divenuta un fatto posto a fondamento dell'atto. La formazione dell'operatore e la presentazione stessa degli output assumono rilievo perché una percentuale o una lista di candidati può orientare il giudizio prima della motivazione.

Qui il rischio non è soltanto che l'operatore ratifichi il risultato, ma che la forma numerica del suggerimento gli trasmetta una certezza che il sistema non possiede. Un punteggio eventualmente esposto non coincide, senza ulteriori informazioni, con la probabilità che la persona segnalata sia quella cercata. La revisione qualificata deve riguardare anche il significato attribuito all'output: quale domanda tecnica ha ricevuto il sistema e quale conclusione giuridica se ne vuole ricavare. Il decreto non prescrive un modello uniforme di motivazione; un atto che trasformi una somiglianza in identificazione certa senza spiegare il passaggio porrebbe però un problema di attendibilità e di controllo.

L'art. 5 individua una base giuridica per il trattamento di dati personali nelle sperimentazioni normative quando sia necessario per finalità di polizia. La base non dispensa dall'osservanza delle condizioni cumulative dell'art. 59, par. 1, del regolamento europeo. Il coinvolgimento del Garante, quando la sperimentazione comporta dati personali, il raccordo con le autorità nazionali e la riserva delle responsabilità sul trattamento alle amministrazioni competenti rendono lo spazio di sperimentazione una sede regolata, non un'area franca. Il successivo regolamento previsto dal comma 4 dovrà definire il coordinamento con lo spazio di sperimentazione di cui all'art. 57 del regolamento europeo. Anche qui la funzione dell'eccezione sperimentale si comprende soltanto mantenendo visibile il soggetto che dispone dei dati e risponde del loro uso.

La sperimentazione consente di misurare affidabilità e limiti prima dell'impiego stabile, ma non sospende le regole sul trattamento dei dati né la responsabilità delle amministrazioni competenti. La medesima continuità fra

preparazione e uso spiega la formazione disciplinata dall'art. 6. I corsi presso gli istituti delle Forze di polizia devono riguardare il funzionamento dei sistemi, i loro limiti, i bias, gli errori, il riconoscimento biometrico, l'analisi predittiva, la lettura critica degli output, le implicazioni giuridiche e la sicurezza informatica. Per i sistemi ad alto rischio alcuni risultati formativi sono richiesti nell'ambito di corsi specifici. La competenza necessaria a interpretare un confronto facciale non coincide in ogni aspetto con quella richiesta per convalidare un modello o motivare un provvedimento: è una esigenza ricavabile dallo scopo della disposizione, mentre il programma dei corsi spetta alle amministrazioni nell'ambito delle risorse disponibili.

Il Garante, esaminando lo schema nel luglio 2026, aveva proposto di sostituire nell'art. 3, comma 4, l'espressione «revisione umana qualificata» con «sorveglianza umana», ritenuta più ampia. Il testo definitivo conserva la prima espressione nel comma 4 e la seconda nel comma 5. Il dato non autorizza a dire che il legislatore abbia ignorato la sorveglianza: essa è espressamente prevista per i sistemi ad alto rischio. Consente, piuttosto, di osservare che la legge mantiene due piani di intervento umano, sui risultati e sul sistema, i cui rapporti dovranno essere chiariti nella prassi.⁸

La distinzione fra revisione del risultato e sorveglianza del sistema diviene più esigente quando l'output non si limita a suggerire una priorità, ma indica il volto di una persona. Per questo il decreto passa dalle regole comuni sull'uso della tecnologia a quelle, più restrittive, dell'identificazione biometrica.

5. Il volto e la prevenzione: identificazione biometrica in tempo reale

Vi è una soglia fra ordinare un insieme di dati biometrici e cercare una persona fra coloro che attraversano uno spazio pubblico. L'art. 7 riguarda il primo momento: consente etichettatura, filtraggio e categorizzazione di set legalmente acquisiti per finalità di polizia, esclude la deduzione delle caratteristiche protette indicate dall'art. 5, par. 1, lett. g), del regolamento europeo e vieta che il risultato sia l'unico fondamento di una decisione produttiva di effetti giuridici. Il trattamento del set non costituisce, dunque, un titolo generale per identificare chi si trovi in un luogo pubblico. Il salto fra le due operazioni spiega la disciplina specifica dell'art. 8.

L'art. 8 riguarda l'identificazione biometrica remota in tempo reale in luoghi pubblici o aperti al pubblico. Per la prevenzione rinvia al punto ii) dell'art. 5, par.

⁸ Garante per la protezione dei dati personali, parere n. 531 del 14 luglio 2026, relativo allo *schema* di decreto, parte «Ritenuto» e dispositivo, lett. a): testo online. Il confronto è svolto con l'art. 3, commi 4 e 5, del testo definitivo.

1, primo comma, lett. h), del regolamento europeo: il rinvio importa il carattere specifico, sostanziale e imminente della minaccia alla vita o all'incolumità fisica, oppure la minaccia terroristica nei termini stabiliti dalla fonte dell'Unione. Per la protezione di persone determinate richiama invece il punto i): ricerca di persone scomparse e di specifiche persone offese da sequestro, tratta o sfruttamento sessuale. Non si può ricavare dall'espressione nazionale «finalità di prevenzione» un potere più ampio di quello circoscritto dal rinvio europeo. L'art. 359-ter c.p.p., richiamato in apertura, governa l'impiego nel procedimento penale e deve essere esaminato separatamente.⁹

L'uso è limitato alla conferma dell'identità o alla ricerca mirata, anche dinamica e comprensiva della localizzazione, di persone specificamente individuate o individuabili rispetto alla minaccia o alla ricerca. Per ogni utilizzo si forma un set di confronto pertinente alla singola finalità, con dati provenienti da archivi legalmente accessibili o da elementi acquisiti lecitamente nell'attività di polizia. I dati biometrici che lo compongono devono essere cancellati al termine dell'autorizzazione e il set non può accrescersi sommando le autorizzazioni passate. Sono vietati gli archivi alimentati mediante scraping non mirato o costituiti in violazione delle norme sulla protezione dei dati. La delimitazione non è un adempimento contabile: riduce il numero delle persone coinvolte nel confronto e rende identificabile il rapporto fra bisogno operativo e trattamento.

Il regolamento europeo richiede, inoltre, di considerare la natura della situazione, la gravità, la probabilità e la portata del danno che si vuole evitare, insieme alle conseguenze della ricerca per i diritti di tutte le persone interessate. Questi parametri impediscono di ridurre la proporzionalità alla formula secondo cui «un sistema utile è un sistema necessario». L'utilità di localizzare una persona non dimostra che sia indispensabile scandagliare un'area estesa per quindici giorni; l'esistenza di una minaccia non dimostra che qualunque banca dati sia adeguata; il carattere mirato della lista di persone ricercate non rende irrilevante l'esposizione delle persone che transitano nell'area ripresa. L'autorizzazione è specifica proprio perché deve dare una risposta a tali domande nel contesto della singola operazione.

L'autorità che richiede l'uso è il questore, il comandante provinciale dell'Arma dei carabinieri o della Guardia di finanza, ovvero il responsabile dei servizi centrali indicati dall'art. 8, comma 4. La richiesta è rivolta al procuratore della Repubblica presso il tribunale del capoluogo del distretto nel quale sono emerse le esigenze di prevenzione o ricerca. Devono essere indicati finalità, durata, area,

⁹ D.lgs. n. 160 del 2026, art. 8, comma 1; Reg. (UE) 2024/1689, art. 5, par. 1, primo comma, lett. h), punti i) e ii). Testo e condizioni delle eccezioni nel portale istituzionale: [testo online](#).

persone, banca dati e tecnologia. L'autorizzazione riguarda uno specifico evento o un tempo strettamente necessario, comunque non superiore a quindici giorni, con possibili proroghe motivate di quindici giorni se permangono le condizioni. Richiede la previa valutazione prevista dall'art. 5, par. 2, del regolamento europeo. La competenza del procuratore in questa sequenza preventiva non va scambiata con quella del giudice per le indagini preliminari prevista dall'art. 359-ter c.p.p. per le ricerche svolte nel procedimento penale.

Il confronto con l'art. 5, par. 3, del regolamento europeo apre una questione ulteriore: la fonte unionale richiede una autorizzazione preventiva rilasciata da un'autorità giudiziaria oppure da un'autorità amministrativa indipendente con decisione vincolante, su richiesta motivata, salvo urgenza giustificata. La qualificazione del procuratore della Repubblica indicato dall'art. 8 rispetto alla nozione unionale di autorità giudiziaria merita di essere condotta tenendo conto della sua posizione istituzionale e delle garanzie effettive della decisione; non la si può liquidare assumendo che ogni ufficio chiamato «giudiziario» soddisfi automaticamente la nozione europea, né affermare qui, senza una verifica specifica, una incompatibilità del modello nazionale. Ciò che il testo rende certo è la differenza interna rispetto alla riserva al giudice prevista dall'art. 359-ter per il procedimento penale. Il rapporto con il requisito europeo resta un tema interpretativo distinto, sul quale la concreta motivazione dell'autorizzazione e la possibilità di controllo assumono rilievo.

Sul piano applicativo la competenza formale non rende, da sola, sostanziale il controllo. Il provvedimento che indichi un evento e ripeta il limite di quindici giorni lascerebbe ancora da spiegare perché l'area prescelta, la durata effettiva e la banca di confronto siano commisurate a quella minaccia o a quella ricerca. Questo contenuto della motivazione è una lettura dei requisiti di specificità e delle valutazioni imposte dall'art. 8 e dall'art. 5 del regolamento, da verificare nel singolo caso; non è una formula ulteriore scritta nel decreto. I log consentiranno un controllo successivo, ma non possono creare retrospettivamente le ragioni che dovevano precedere l'attivazione.

Nell'urgenza, l'organo di polizia può avviare il sistema su disposizione dei responsabili individuati dalla norma, previa comunicazione anche orale al procuratore, quando il ritardo rischi di causare un pregiudizio grave e irreparabile alle finalità ammesse. La richiesta deve seguire senza ritardo e comunque entro ventiquattro ore dall'inizio; il procuratore decide nelle successive ventiquattro ore. L'area e le persone ricercate devono essere delimitate anche in questa fase. Se non sono rispettate le condizioni o i termini dei commi 4-7, oppure l'autorizzazione manca, l'uso cessa immediatamente; dati, risultati e output sono cancellati, con la sola salvezza degli elementi acquisiti

legittimamente sotto un'altra base giuridica conforme al d.lgs. n. 51 del 2018. I risultati ottenuti in violazione dell'art. 8 non possono essere utilizzati. L'eccezione relativa all'altra base giuridica non dovrebbe trasformarsi, sul piano interpretativo, in uno strumento per conservare il risultato della ricerca illecita semplicemente mutandone la denominazione.¹⁰

L'art. 8, comma 9, richiama inoltre l'art. 226, comma 5, disp. att. c.p.p.: gli elementi acquisiti attraverso attività preventive non possono essere utilizzati nel procedimento penale, fatti salvi i fini investigativi, secondo il regime della norma richiamata. Bisogna tenere distinti due limiti. Il primo riguarda il risultato prodotto in violazione delle condizioni dell'art. 8; il secondo riguarda, anche quando la ricerca preventiva sia stata regolarmente autorizzata, la sua circolazione nell'ambito del procedimento penale. Una informazione può orientare una successiva indagine senza diventare, per questo, una prova liberamente spendibile. L'eventuale elemento successivamente acquisito dovrà avere la propria base legale e la propria verificabilità.

Completa la disciplina l'art. 9. Il titolare del trattamento compie preventivamente sia la valutazione d'impatto sui diritti fondamentali prevista dal regolamento europeo sia quella relativa alla protezione dei dati prevista dagli artt. 23 e 24 del d.lgs. n. 51 del 2018. Ogni utilizzo è registrato in file di log non modificabili, conservati per cinque anni e accessibili alle autorità competenti per il controllo della liceità, il controllo interno o un procedimento penale; restano distinti i termini di conservazione dei dati trattati per finalità di polizia. Dopo l'uso il titolare notifica l'attivazione al Garante, con previo nulla osta dell'autorità giudiziaria che può differirlo per esigenze di segretezza nei limiti indicati, senza comunicare dati operativi sensibili. Un decreto ministeriale dovrà definire requisiti tecnici, accuratezza, controllo dei bias, qualità delle basi di confronto e modalità della notifica. La conservazione del log per cinque anni e la conservazione dei dati personali trattati sono grandezze giuridiche differenti: confonderle significherebbe prolungare senza titolo la disponibilità di immagini e profili biometrici.¹¹

Le due valutazioni d'impatto hanno oggetti che si intersecano senza coincidere: l'una considera la posizione complessiva delle persone rispetto all'uso del sistema, l'altra i rischi del trattamento dei dati. Anche la notifica al Garante, che può essere differita per esigenze di segretezza fino a tre mesi, rinnovabili una sola volta, risponde a una funzione diversa dall'autorizzazione preventiva. L'insieme

¹⁰ D.lgs. n. 160 del 2026, art. 8, commi 4-8. Il Garante, sullo schema, aveva chiesto di circoscrivere l'eccezione dell'«altra base giuridica»: parere n. 531 del 2026, parte «Ritenuto», disponibile all'indirizzo della nota 9. Il testo definitivo va letto per ciò che stabilisce, senza attribuirgli una restrizione testuale ulteriore.

¹¹ D.lgs. n. 160 del 2026, art. 9, commi 1-5; artt. 23 e 24 d.lgs. n. 51 del 2018; d.P.R. 15 gennaio 2018, n. 15, art. 10.

di questi controlli riguarda l'uso preventivo del sistema. Se la ricerca si colloca invece in un procedimento penale, mutano l'autorità che autorizza e, soprattutto, la sorte processuale del risultato.

6. La ricerca nel procedimento penale

La medesima tecnologia assume una collocazione diversa quando la ricerca è compiuta nell'ambito di un procedimento penale. L'art. 13 inserisce nel codice di procedura penale l'art. 359-ter per l'identificazione o localizzazione biometrica remota in tempo reale durante l'attività investigativa. Non basta più richiamare una esigenza preventiva; la ricerca deve corrispondere a una delle ipotesi tipizzate e il pubblico ministero si rivolge, ordinariamente, al giudice per le indagini preliminari. Il mutamento di sede non riguarda soltanto l'autorità competente: investe i presupposti e l'ingresso del risultato nel materiale utilizzabile nel processo.¹²

Il comma 1 consente di confermare l'identità di una persona nei confronti della quale sussistono «sufficienti indizi» della commissione di uno dei delitti elencati nell'allegato II del regolamento europeo, puniti con la reclusione il cui massimo non è inferiore a quattro anni. Consente, alle stesse condizioni, la ricerca mirata e la localizzazione della persona indiziata. La formula «sufficienti indizi» non può essere sostituita senza base testuale con quella dei «gravi indizi» propria di altri istituti. Occorre inoltre che il reato appartenga al catalogo europeo e raggiunga la soglia edittale nazionale: la gravità attribuita in concreto al fatto non supplisce alla mancanza dell'una o dell'altra condizione.

Il comma 2 riguarda il latitante ricercato per eseguire una misura cautelare coercitiva o un ordine di carcerazione non sospeso, sempre in relazione ai delitti indicati dal comma 1. La latitanza e il titolo da eseguire non autorizzano una ricerca biometrica per qualunque reato. Il comma 4 ammette, con le modalità dei commi precedenti, la ricerca mirata di «specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani» nell'ambito di un procedimento penale. Si conserva qui il lessico testuale della disposizione. L'art. 8 parla, nella distinta sede preventiva, di persona scomparsa e di vittime di sequestro, tratta o sfruttamento sessuale; il comma 4 dell'art. 359-ter impiega la parola «sottrazione». L'interprete potrà interrogarsi sull'estensione delle due formule, ma non dovrà presentarle come identiche.

Il confronto si svolge su una banca dati adeguata alla specifica ricerca, composta per ciascun utilizzo con i soli dati pertinenti e cancellati al termine

¹² D.lgs. n. 160 del 2026, art. 13, che introduce l'art. 359-ter c.p.p. Testo ufficiale: testo online. Si veda anche l'allegato II al Reg. (UE) 2024/1689: testo online.

dell'autorizzazione; non è consentito accumulare i set precedenti né ricorrere ad archivi generati con scraping non mirato o costituiti illecitamente. Le immagini e gli altri elementi biometrici possono provenire anche dalle indagini, purché acquisiti legalmente. Il punto è decisivo per la controllabilità dell'operazione. Una identificazione non è verificabile se si conosce soltanto il risultato del confronto e resta ignota la composizione dell'archivio sul quale il sistema lo ha compiuto. Provenienza della traccia, dimensioni del set, criteri di inclusione e dati di confronto sono parte della spiegazione del risultato; non costituiscono, per il solo fatto di essere tecnici, informazioni giuridicamente irrilevanti.

Questa esigenza tocca direttamente il diritto di difesa. Per contestare un'identificazione occorre sapere se il sistema abbia semplicemente segnalato un candidato o se abbia prodotto un'affermazione presentata come certa; occorre verificare la qualità della traccia originaria e l'eventuale presenza di altri candidati compatibili. Non ne deriva che ogni dettaglio riservato del sistema debba essere divulgato senza limiti in qualsiasi fase. Deriva, piuttosto, che la difesa non può essere confinata alla contestazione di una conclusione priva dei presupposti indispensabili per valutarla. Le regole sulla documentazione dell'attività, sulla conservazione dei log e sull'accesso agli atti dovranno essere coordinate con tale esigenza nel procedimento concreto. Il decreto non detta una disciplina completa del contraddittorio tecnico: riconoscere questo limite del testo è diverso dal presumere che il risultato sia insindacabile.

Una lista di candidati prodotta dal sistema, per ipotesi, è un invito ad accertare, non un accertamento dell'identità. Se una persona è selezionata perché compare in testa alla lista, la qualità delle immagini e il modo in cui è stato costruito il confronto contano per valutare la forza del risultato; un punteggio non equivale, da solo, alla probabilità processuale dell'identificazione. Da questa cautela non discende una regola automatica di inutilizzabilità. Occorre distinguere la liceità dell'acquisizione, l'attendibilità tecnica del confronto e il valore dell'inferenza alla luce degli elementi indipendenti. Sono giudizi diversi, che possono condurre a esiti diversi e che l'atto fondato sulla ricerca dovrebbe rendere riconoscibili.

L'autorizzazione ordinaria è chiesta dal pubblico ministero al giudice per le indagini preliminari. Il giudice provvede con decreto motivato, delimitando area geografica, persone ricercate e durata strettamente necessaria, non superiore a quindici giorni; può prorogarla, su richiesta del pubblico ministero e con nuova motivazione, per successivi periodi di quindici giorni se le condizioni permangono. Le valutazioni richieste dall'art. 5, par. 2, del regolamento europeo devono precedere l'autorizzazione. Il controllo del giudice investe così l'utilità della ricerca, il suo oggetto e il sacrificio imposto a chi si trovi nello spazio

interessato. L'individuazione di una persona specifica non rende invisibili tutte le altre le cui immagini sono tecnicamente sottoposte al sistema.

L'urgenza è disciplinata dal comma 7 mediante due percorsi. Se non si può attendere il giudice, il pubblico ministero dispone l'uso con decreto motivato, immediatamente comunicato e comunque trasmesso entro ventiquattro ore al giudice, che nelle successive quarantotto ore convalida, quando ne ricorrono i presupposti, e autorizza la prosecuzione. Se neppure il provvedimento del pubblico ministero è attendibile, gli ufficiali di polizia giudiziaria avviano il sistema; trasmettono la richiesta al pubblico ministero senza ritardo e comunque entro dodici ore, il pubblico ministero chiede la convalida al giudice entro ventiquattro ore dall'avvio, e il giudice provvede nelle successive quarantotto ore. In entrambi i casi l'urgenza richiede un fondato motivo di temere un pregiudizio grave e irreparabile per le finalità dei commi 1-4. Le scansioni temporali non si riducono a un unico termine di quarantotto ore e non sono intercambiabili con quelle dell'art. 8.

Il comma 8 stabilisce che i risultati non possono essere utilizzati se il sistema è impiegato fuori dei casi consentiti dalla legge o senza osservare i commi 6 e 7. Impone inoltre la cancellazione di dati, risultati e output, fatta salva la loro eventuale natura di corpo del reato. È una conseguenza espressamente prevista per il risultato dell'attività: chiamarla genericamente «nullità dell'autorizzazione» farebbe perdere la distinzione fra vizi dell'atto e divieto di impiego del materiale ottenuto. La norma non risolve, peraltro, ogni problema relativo agli atti investigativi successivi. La legittimità di un elemento ulteriore dovrà essere valutata secondo la sua genesi concreta e le disposizioni applicabili, senza postulare una automatica propagazione dell'inutilizzabilità né una automatica sanatoria mediante acquisizioni derivate. L'art. 9 del decreto aggiunge a questo percorso le due valutazioni di impatto, i log, la notifica e le garanzie tecniche comuni alle forme di identificazione in tempo reale.

La portata della clausola «fuori dei casi consentiti dalla legge» dovrà essere stabilita in rapporto al vizio dedotto. La ricerca per un delitto estraneo al catalogo, l'inclusione di persone non comprese nell'autorizzazione e il superamento dei limiti territoriali richiedono ciascuno un accertamento specifico; la norma menziona inoltre espressamente la violazione dei commi 6 e 7. Non ogni difetto tecnico riceve automaticamente la medesima conseguenza processuale. Questo punto distingue la contestazione della liceità dell'acquisizione da quella dell'affidabilità del risultato. Il decreto regola separatamente, infine, un altro modo di cercare un volto: il confronto effettuato dopo l'acquisizione delle immagini.

7. Il riconoscimento facciale a posteriori

L'intervallo fra la ripresa e il confronto cambia il regime della ricerca, ma solo quando è reale. L'art. 10 ammette che un sistema di videosorveglianza, installato in base a una disposizione di legge, sia integrato con componenti di intelligenza artificiale; il riconoscimento facciale può attivarsi dopo l'acquisizione delle immagini, nelle ipotesi dei commi 2 e 3. Un ritardo artificiosamente breve non trasformerebbe una identificazione in tempo reale in una ricerca a posteriori: il regolamento europeo comprende nella prima categoria anche differimenti utilizzati per eluderne i limiti. La sequenza concreta di acquisizione, confronto e individuazione della persona conta più dell'etichetta attribuita al programma.¹³

Nella regola generale del comma 2 la ricerca è mirata a una persona indiziata della commissione di un reato. Gli ufficiali di polizia giudiziaria che hanno avviato i sistemi presentano istanza al pubblico ministero; quest'ultimo chiede l'autorizzazione al giudice per le indagini preliminari senza ritardo e comunque entro quarantotto ore dall'avvio; il giudice decide con decreto motivato nelle quarantotto ore successive. Il richiamo europeo all'autorizzazione preventiva o tempestivamente successiva, contenuto nell'art. 26, par. 10, aiuta a leggere la struttura della norma nazionale. Se il pubblico ministero non osserva il termine o l'autorizzazione manca, l'uso della tecnologia collegato a quella richiesta cessa immediatamente e dati, risultati e output sono cancellati, salvo che costituiscano corpo del reato. Il comma 2 non adopera, in questa ipotesi, la medesima formula espressa di «non utilizzazione dei risultati» che compare nel comma 3: occorre riportare fedelmente la conseguenza prevista, ferma la rilevanza processuale dell'obbligo di cancellazione e delle altre regole applicabili.

Il comma 3 sottrae all'autorizzazione del giudice un caso circoscritto: l'identificazione iniziale, dopo la commissione del reato, di una persona potenzialmente indiziata, fondata su elementi oggettivi e verificabili direttamente connessi al fatto. L'uso ricade allora sotto la diretta ed esclusiva responsabilità dell'ufficiale di pubblica sicurezza designato dal questore per la gestione dell'ordine e della sicurezza pubblica oppure, fuori da tale ipotesi, dell'ufficiale di polizia giudiziaria di cui all'art. 57, comma 1, lett. a) e b), c.p.p. che procede in relazione al reato. La finalità esclusiva e la base fattuale già disponibile delimitano l'eccezione: non basta chiamare «iniziale» una ricerca estesa a persone o fatti ulteriori. Se le condizioni del comma 3 non sono osservate, i risultati non possono essere utilizzati e dati, risultati e output sono cancellati, salvo che costituiscano corpo del reato.

¹³ D.lgs. n. 160 del 2026, art. 10, commi 1-3; Reg. (UE) 2024/1689, art. 3, punti 42) e 43), e art. 26, par. 10.

La distinzione fra identificazione iniziale e ricerca di un indiziato non è sempre immediata sul piano materiale. L'ufficiale può servirsi del sistema per attribuire un nome a una persona ripresa durante un fatto; dopo quel primo risultato può volere ampliare la ricerca ad altri filmati, luoghi o persone. La prima operazione, se soddisfa tutti i requisiti del comma 3, non richiede l'autorizzazione del comma 2; la seconda non eredita automaticamente la medesima esenzione. Il criterio è la finalità esclusiva dell'identificazione iniziale, insieme al legame diretto con elementi oggettivi già verificabili. In assenza di questa delimitazione l'eccezione rischierebbe di assorbire la regola, perché quasi ogni ricerca può essere descritta retrospettivamente come un primo tentativo di individuare qualcuno.

Il problema delle immagini raccolte prima del reato emerge nel comma 4. Nei luoghi o eventi individuati secondo i criteri demandati a un decreto del Ministro dell'interno, le immagini del volto dei presenti sono trattate automaticamente e memorizzate in una base locale «senza elaborazione dei relativi dati biometrici». Vi possono essere associati dati anagrafici e, ove previsto, l'identificativo del posto risultanti dalla scansione dei titoli di accesso. Soltanto dopo la commissione di un reato l'attivazione del riconoscimento comporta l'elaborazione biometrica delle immagini conservate e il confronto mirato. La raccolta anticipata dei titoli di accesso e delle immagini resta nondimeno un trattamento di dati personali di una platea potenzialmente ampia. La separazione temporale dell'elaborazione biometrica riduce il rischio di identificazione generalizzata, ma non elimina la necessità della base legale per la videosorveglianza e di criteri proporzionati per scegliere luoghi ed eventi.

Si pensi a un evento al quale accedano molte persone con un titolo nominativo. Nessun reato è ancora avvenuto e il confronto biometrico non è attivo; intanto, però, immagini e dati di accesso sono stati raccolti. Il differimento dell'elaborazione biometrica è una garanzia effettiva rispetto all'identificazione immediata, ma non risponde alla domanda anteriore: perché era necessario costituire quella base per quell'evento? È qui che i criteri demandati al decreto ministeriale e la valutazione preventiva del trattamento dovranno mostrare la propria capacità selettiva. Il termine di sette giorni previsto dall'art. 10, comma 7, limita la conservazione; non dimostra, da solo, la necessità della raccolta iniziale.

Il Garante aveva osservato sullo schema che un'elaborazione biometrica preventiva di tutti i partecipanti a un evento sarebbe difficilmente conciliabile con la ricerca mirata a posteriori. Nel testo definitivo il comma 4 distingue espressamente la memorizzazione preliminare delle immagini dall'elaborazione biometrica successiva alla commissione del reato. È un mutamento da registrare; non autorizza a sostenere che ogni questione sollevata dal Garante sia risolta. L'ampiezza dei luoghi e degli eventi ammessi, i criteri demandati alla fonte

ministeriale e il rapporto fra raccolta generalizzata delle immagini e ricerca individuale restano oggetto di una valutazione di proporzionalità nel caso concreto.¹⁴

Il Ministero dell'interno è titolare del trattamento; prima dell'impiego deve effettuare la valutazione d'impatto sulla protezione dei dati e consultare il Garante ai sensi degli artt. 23 e 24 del d.lgs. n. 51 del 2018, con possibilità di una valutazione unica per sistemi analoghi. I dati personali nella base locale si conservano per sette giorni dalla raccolta, mentre i log non modificabili degli accessi e delle operazioni si conservano per cinque anni: ancora una volta, non si tratta del medesimo archivio né del medesimo termine. Il comma 10 vieta decisioni con effetti giuridici negativi basate unicamente sul risultato del riconoscimento e richiama le garanzie dell'art. 8 del d.lgs. n. 51 del 2018; il comma 11 vieta riconoscimenti non mirati e identificazioni generalizzate o indiscriminate. L'installazione e la manutenzione possono essere curate, alle condizioni del comma 13, da gestori e organizzatori, ma il sistema è concesso in comodato gratuito alla questura, che ne acquisisce la disponibilità completa ed esclusiva. La partecipazione materiale di un privato alla infrastruttura non gli attribuisce il potere di decidere chi identificare.

La durata di sette giorni tutela anche chi non diventerà mai oggetto di indagine; non può essere aumentata informalmente per evitare la perdita di immagini potenzialmente utili. Fin qui il decreto ha riguardato le condizioni per usare il sistema e per conservare i suoi risultati. Il titolo II pone una domanda diversa: che cosa accade quando la sicurezza del sistema viene compromessa da una condotta umana e ne deriva un pericolo penalmente rilevante?

8. Pericolo, colpevolezza e responsabilità dell'ente

Il passaggio dalla disciplina dell'uso alla fattispecie penale esige di cambiare oggetto dell'accertamento. Nell'art. 437-bis c.p., introdotto dall'art. 12 del decreto, il fatto non consiste nell'errore del sistema: consiste nell'omissione di misure dovute, nell'alterazione del sistema oppure, per l'utilizzatore professionale, nell'omissione intenzionale della sorveglianza. Da queste condotte deve derivare il pericolo descritto dalla norma per la vita o l'incolumità pubblica o individuale, oppure per la sicurezza dello Stato. Il sistema ad alto rischio individua l'ambito della fattispecie; da solo non prova la condotta, il pericolo o il loro collegamento causale.¹⁵

¹⁴ Garante, parere n. 531 del 2026, parte «Ritenuto», in particolare sul trattamento preventivo delle immagini nei luoghi ed eventi: indirizzo alla nota 9. Per il testo definitivo, d.lgs. n. 160 del 2026, art. 10, commi 4 e 12.

¹⁵ D.lgs. n. 160 del 2026, art. 12, che inserisce l'art. 437-bis c.p.: testo online. Il requisito del «pericolo concreto» compare nella delega: l. n. 132 del 2025, art. 24, comma 5, lett. b).

Il primo comma riguarda chi omette misure tecniche di sicurezza previste per progettazione, addestramento, produzione e immissione sul mercato di sistemi ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni, oppure omette misure di sorveglianza umana. La pena è della reclusione da uno a cinque anni se deriva pericolo per la vita o l'incolumità; sale da due a otto anni se deriva pericolo per la sicurezza dello Stato. Il testo dice «chiunque», ma un reato omissivo presuppone l'individuazione della misura dovuta e del soggetto al quale spettava adottarla. Né il carattere diffuso di una filiera tecnologica né la molteplicità dei suoi operatori autorizzano una imputazione indistinta: occorre ricostruire il ruolo concreto di ciascuno, la sua capacità di intervento e il segmento del processo sul quale esercitava un controllo effettivo.

La descrizione della condotta rinvia a fasi diverse del ciclo del sistema. Una carenza nella progettazione non è la stessa omissione di una misura durante l'addestramento; la messa in circolazione di una versione non corretta pone questioni differenti dall'uso professionale di un sistema già installato. Per ciascuna fase occorrerà identificare le misure tecniche previste e il rapporto che esse avevano con la prevenzione del tipo di malfunzionamento o di alterazione verificatosi. Il giudizio controfattuale sull'omissione non può essere sostituito dalla constatazione che, dopo il fatto, una precauzione ulteriore sarebbe stata astrattamente possibile. La norma incrimina l'omissione di misure dovute e causalmente connesse al pericolo, non l'impossibilità di garantire un sistema infallibile.

Anche i beni protetti richiedono una lettura distinta. Il pericolo per la vita o l'incolumità individuale può riguardare una persona determinata; quello per l'incolumità pubblica implica una dimensione diversa dell'esposizione al rischio; il pericolo per la sicurezza dello Stato comporta una cornice offensiva ulteriore e una pena maggiore. Non sarebbe metodologicamente corretto elevare ogni difetto di cybersicurezza a pericolo per lo Stato in ragione della sola diffusione di un sistema informatico. Le condizioni tecniche dell'attacco o del malfunzionamento e le possibili conseguenze istituzionali andranno provate. Simmetricamente, una violazione che riguardi un singolo individuo non perde rilevanza perché non mette in pericolo una pluralità indeterminata di persone: il testo include espressamente l'incolumità individuale.

Il secondo comma, fuori dai casi del primo e salva la più grave fattispecie, punisce l'alterazione di sistemi ad alto rischio se ne deriva il pericolo indicato, con pene da due a sei anni o, per la sicurezza dello Stato, da tre a dieci anni. L'alterazione è una condotta commissiva distinta dall'omessa adozione delle misure. Il terzo comma contempla soltanto i fatti del primo comma commessi per colpa grave, riducendo la pena da un terzo a un sesto; non estende una

responsabilità colposa all'alterazione del secondo comma né alla figura dell'utilizzatore professionale del quarto. Quest'ultima punisce l'omissione «intenzionale» delle misure di sorveglianza umana quando ne derivi il pericolo descritto, rinviando alle pene del primo comma. Per attribuire il fatto non basta individuare la posizione professionale o il risultato pericoloso: occorre accertare la condotta omissiva intenzionale nei termini propri della fattispecie.

La legge delega, all'art. 24, comma 5, lett. b), aveva menzionato un «pericolo concreto» per vita, incolumità o sicurezza dello Stato. Nel testo dell'art. 437-bis l'aggettivo non compare, mentre è richiesta la derivazione del pericolo dalle omissioni o dall'alterazione. Una lettura che esiga l'accertamento di un pericolo effettivo, riferibile alle circostanze del fatto, appare coerente con la delega e con la struttura causale della norma; resta una proposta interpretativa, non la citazione di una parola contenuta nel precetto. La prova non potrà limitarsi a evocare astrattamente la pericolosità dell'intelligenza artificiale. Dovrà precisare la misura omessa, la funzione preventiva che essa avrebbe svolto, il modo in cui il sistema è divenuto pericoloso e il rapporto con la condotta dell'imputato.

La successione delle fonti europee rende questo accertamento più esigente. L'obbligo al quale il precetto penale fa riferimento dev'essere determinabile e applicabile nel tempo del fatto, anche quando la classificazione del sistema come ad alto rischio sia già riconoscibile. Il differimento di parte degli obblighi europei disposto nel 2026 non può essere ignorato; neppure consente di concludere, in blocco, che ogni cautela nazionale sia sospesa. Per la norma penale il principio di legalità richiede una ricostruzione puntuale del dovere richiamato, della sua fonte e della sua esigibilità. Come per ogni nuova incriminazione, inoltre, l'art. 25, secondo comma, Cost. e l'art. 2 c.p. impediscono di applicarla retroattivamente a fatti anteriori alla sua entrata in vigore.

Nell'accertamento del profilo soggettivo sarà altrettanto necessario distinguere la conoscenza del rischio dalla possibilità concreta di impedirlo. La prova che un responsabile abbia ricevuto un rapporto tecnico non equivale a dimostrare che disponesse del potere di adottare la misura omessa; la prova che un operatore potesse interrompere l'uso non dimostra che conoscesse il difetto che rendeva l'interruzione necessaria. Il quarto comma seleziona l'omissione intenzionale dell'utilizzatore professionale, mentre il terzo delimita la colpa grave riferendola ai fatti del primo. Una contestazione che non identifichi il comma applicato e il contributo del singolo soggetto rischierebbe di sovrapporre figure che la norma ha tenuto separate. L'architettura complessa del sistema non autorizza a semplificare la colpevolezza.

La scelta di incriminare il governo difettoso delle condizioni di sicurezza, anziché l'errore del sistema in quanto tale, permette di cercare una condotta umana determinata. Presenta tuttavia un punto vulnerabile: una parte delle misure richiamate dipende da fonti tecniche esterne e dalla loro decorrenza. Dopo un incidente sarà facile indicare una precauzione che avrebbe potuto evitarlo; più difficile, e giuridicamente indispensabile, provare che proprio quella misura fosse dovuta a quel soggetto al momento del fatto e che dalla condotta sia derivato il pericolo tipizzato. Questa verifica impedisce di trasformare l'art. 437-bis c.p. in una clausola generale di punizione del malfunzionamento. È su tale confine, più che sull'astratta severità delle pene, che si misurerà la tenuta della nuova fattispecie.

L'art. 15 inserisce nel d.lgs. 8 giugno 2001, n. 231, l'art. 25-vicies. Per il delitto dell'art. 437-bis c.p. prevede una sanzione pecuniaria da seicento a mille quote; per il delitto dell'art. 612-quater c.p. una sanzione da duecento a settecento quote; in entrambi i casi richiama le sanzioni interdittive dell'art. 9, comma 2, lett. b), c), d) ed e). Il reato di diffusione illecita di contenuti falsificati o alterati con sistemi di IA era già stato introdotto dalla legge n. 132 del 2025: il decreto del 2026 lo include fra i reati presupposto dell'ente, non lo istituisce ex novo. La responsabilità dell'ente non discende automaticamente dalla commissione del delitto: rimangono necessari i criteri generali del d.lgs. n. 231 del 2001, fra cui il rapporto fra autore ed ente, l'interesse o vantaggio e le regole sulla sua organizzazione.¹⁶

L'inserimento nel catalogo dei reati presupposto ha un rilievo organizzativo preciso. Nel primo caso l'ente dovrà guardare alla filiera delle misure tecniche, alla designazione delle responsabilità, al controllo delle versioni del sistema e alla sorveglianza dell'impiego professionale; nel secondo, alle condizioni nelle quali immagini, voci e video falsificati possono essere prodotti e diffusi nel suo interesse o a suo vantaggio. Non si può dedurre dal solo possesso di uno strumento generativo la commissione del delitto dell'art. 612-quater c.p., che ha propri elementi costitutivi, né dal solo verificarsi di un guasto la responsabilità dell'ente per l'art. 437-bis. La struttura dei modelli organizzativi rimane legata ai rischi di reato effettivamente riconoscibili e alle condotte umane che li realizzano.

La distinzione fra intervento sul rischio e accertamento della responsabilità ricompare nell'art. 14. La modifica dell'art. 104, comma 1, lett. e-bis), disp. att. c.p.p. riguarda l'esecuzione del sequestro preventivo di contenuti online «generati anche con sistemi di intelligenza artificiale». Essa non introduce un reato né sostituisce i presupposti del sequestro previsti dal codice: rimuovere o

¹⁶ D.lgs. n. 160 del 2026, art. 15; l. n. 132 del 2025, art. 26, comma 1, lett. c), che ha introdotto l'art. 612-quater c.p.: testo online. Per l'imputazione all'ente, d.lgs. n. 231 del 2001, artt. 5-7.

rendere inaccessibile un contenuto è una misura cautelare, mentre attribuirne penalmente la produzione o la diffusione richiede un accertamento ulteriore.¹⁷ La medesima esigenza di distinguere il fatto dalla sua conseguenza attraversa, con strumenti diversi, il capo sulla responsabilità civile: chi afferma di avere subito un danno deve poter ricostruire il funzionamento del sistema senza che la difficoltà della prova equivalga già alla prova della responsabilità.

9. Il danno, la prova e la presunzione causale

Per il danneggiato il primo ostacolo può consistere nel fatto che il sistema appartiene, è gestito o è documentato da altri. Egli conosce la decisione che lo ha colpito, ma non necessariamente i registri o le condizioni tecniche che permetterebbero di ricostruirla. Il capo II del titolo II interviene su questa asimmetria senza creare una responsabilità generale per ogni risultato indesiderato. L'art. 16, comma 1, estende l'accesso alla prova dell'art. 17 alle azioni contrattuali ed extracontrattuali per danni cagionati nell'utilizzo di un sistema di IA; i commi 2 e 3 circoscrivono invece gli artt. 18 e 19 ai danni derivanti dalla violazione di obblighi del regolamento europeo, facendo salvi l'art. 82 del regolamento (UE) 2016/679 e la disciplina nazionale di recepimento della direttiva (UE) 2024/2853.¹⁸

Rimangono da identificare il titolo della domanda e il soggetto che vi deve rispondere. Nell'azione contrattuale occorre ricostruire il rapporto e l'obbligo assunto; in quella extracontrattuale possono venire in considerazione gli artt. 2043, 2050 o 2051 c.c., purché ne sussistano i rispettivi presupposti. Non ogni impiego di IA è, per ciò solo, «attività pericolosa» o esercizio di custodia su una «cosa». Gli artt. 17-19 non risolvono questa qualificazione: modificano le condizioni della prova e impediscono che la conformità regolatoria sia trattata come una esenzione generale dalla responsabilità.

L'art. 17 traduce l'asimmetria informativa in un potere processuale circoscritto. Il giudice, su istanza della parte che allega il danno, ordina all'altra parte o al terzo che ne dispone l'esibizione degli elementi specificamente pertinenti al funzionamento del sistema, quando l'istante presenta fatti ed elementi idonei a rendere verosimile la domanda anche con riferimento al collegamento fra il risultato del sistema e il danno. La parte può dunque ottenere registri o documenti che non possiede, ma deve identificare il fatto da accertare e spiegare

¹⁷ D.lgs. n. 160 del 2026, art. 14; art. 104, comma 1, lett. e-bis), disp. att. c.p.p. nel testo riportato nelle note ufficiali al decreto; art. 321 c.p.p. per i presupposti del sequestro preventivo.

¹⁸ D.lgs. n. 160 del 2026, art. 16, commi 1-4. Il comma 4 attribuisce inoltre competenza al giudice della residenza o del domicilio del danneggiato persona fisica che agisca per scopi estranei alla propria eventuale attività professionale o imprenditoriale; è un foro aggiuntivo, non una trasformazione di ogni azione risarcitoria in controversia di consumo.

la pertinenza del materiale richiesto per quanto le è possibile conoscerlo. La disposizione non accorda un accesso indiscriminato al codice sorgente e non dispensa dall'allegazione del danno.

La norma dice «ordina» quando ricorrono le condizioni che essa stabilisce; il giudice deve quindi valutare verosimiglianza, pertinenza e proporzionalità. Il requisito più delicato è il primo: l'istante non possiede il materiale che chiede di vedere, ma deve offrire fatti esterni al sistema che rendano plausibile il collegamento fra il suo risultato e il danno. La collocazione del sistema nella sequenza dei fatti, l'esistenza di una decisione effettivamente presa con il suo contributo e le informazioni accessibili sugli output possono assumere rilievo. Sono esempi ricostruttivi, non una lista probatoria fissata dal legislatore.

Si consideri una persona che lamenti un danno per il diniego di una prestazione e alleggi il contributo di una classificazione automatizzata. Può documentare il diniego e indicare gli elementi dai quali desume il ruolo del sistema, senza disporre dei log, della versione impiegata o dei criteri di classificazione. Pretendere già questi documenti per ordinare l'esibizione renderebbe la tutela circolare; accontentarsi della sola affermazione che «è stata usata l'IA» renderebbe invece l'ordine esplorativo. La verifica richiesta dall'art. 17 si colloca fra i due estremi: un collegamento fattuale verosimile e documenti individuati per quanto conoscibili dall'esterno. L'esibizione apre l'accertamento, non anticipa il giudizio sulla responsabilità.

I registri dell'art. 12 del regolamento europeo, la documentazione sulla gestione dei rischi dell'art. 9, le informazioni tecniche pertinenti dell'art. 11 e quelle relative alla sorveglianza umana dell'art. 14 costituiscono esempi espressamente indicati dal comma 2. Il giudice limita l'ordine a quanto necessario e proporzionato, bilanciando anche i segreti commerciali e le informazioni riservate; quando occorre adotta le misure di tutela previste, con rinvio all'art. 121-ter del codice della proprietà industriale. L'opacità del sistema non giustifica, dunque, un accesso illimitato a ogni segreto dell'impresa, ma il segreto non può diventare, a sua volta, uno schermo assoluto contro la verifica di una domanda plausibile. La proporzione riguarda sia l'estensione dell'esibizione sia le modalità della sua conoscenza nel processo.¹⁹

L'ordine potrà essere circoscritto, ad esempio, alla versione del sistema e all'intervallo temporale rilevanti per il fatto controverso. La parte istante deve spiegare quale accertamento ne trarrebbe; la tutela del segreto potrà incidere sulle

¹⁹ D.lgs. n. 160 del 2026, art. 17, commi 1-6; d.lgs. 10 febbraio 2005, n. 30, art. 121-ter; art. 116 c.p.c. Per il problema generale dell'opacità delle decisioni fondate su sistemi informatici, cfr. PASQUALE F., *The Black Box Society*, Harvard University Press, Cambridge (Mass.), 2015.

modalità della conoscenza, non trasformarsi nell'obbligo di dimostrare già compiutamente ciò che l'esibizione è destinata a chiarire.

Il regime dell'inadempimento all'ordine distingue il destinatario e l'oggetto della richiesta. Se è la parte a non adempiere senza giustificato motivo, il giudice può desumere argomenti di prova ai sensi dell'art. 116 c.p.c.; se l'inadempimento riguarda i documenti specificamente elencati nel comma 2, dopo avere valutato ogni altro elemento di prova, ritiene ammessi i fatti allegati dall'istante. La seconda conseguenza è più incisiva della prima, ma non rende automaticamente fondata ogni domanda: concerne i fatti allegati e resta inserita nella valutazione del materiale processuale. Se invece è il terzo a non adempiere senza motivo, il giudice lo condanna alla pena pecuniaria da 1.500 a 10.000 euro. Confondere la sanzione del terzo con l'ammissione dei fatti da parte del convenuto altererebbe la disciplina.

L'art. 18 dispone che, quando il danno deriva dalla violazione di obblighi del regolamento europeo, il nesso causale fra violazione e danno si presume salvo prova contraria. La formulazione pone una difficoltà logica. Se si chiedesse al danneggiato di dimostrare compiutamente, prima della presunzione, che il danno «deriva» dalla violazione, la regola sulla causalità non avrebbe un oggetto utile. Una lettura che conservi efficacia alla disposizione richiede di accertare la violazione pertinente e il danno, nonché un collegamento fattuale sufficiente a collocare la pretesa nell'ambito dell'art. 16, comma 2; è poi la relazione causale specificamente indicata dall'art. 18 a essere presunta, salva la prova contraria. Questa ricostruzione è interpretativa. Il decreto non definisce in modo analitico il livello di plausibilità del collegamento richiesto per attivarla, mentre l'art. 17 disciplina separatamente la soglia per ottenere l'esibizione. Le due disposizioni non vanno fuse in una sola regola di inversione dell'onere probatorio.

La presunzione è inoltre relativa. Il convenuto può provare che, pur essendo stato violato un obbligo europeo, il danno sarebbe comunque derivato da una causa indipendente o che quella violazione non ha inciso sul percorso causale allegato. L'oggetto preciso della prova contraria dipenderà dal fatto controverso; non è lecito predeterminarlo in una formula unica per tutti i sistemi. L'art. 18 alleggerisce la posizione probatoria del danneggiato sul nesso indicato, ma non stabilisce una responsabilità oggettiva per ogni non conformità, non presume l'entità del danno e non individua da solo il soggetto passivamente legittimato. La distanza fra assistenza alla prova e creazione del titolo della responsabilità deve rimanere visibile.

L'art. 19 aggiunge che la conformità del sistema agli obblighi del regolamento europeo, anche certificata secondo la relativa disciplina, non esclude «di per sé»

la responsabilità del convenuto. Non afferma che la conformità sia irrilevante in ogni giudizio; impedisce che essa diventi una immunità generale. Un sistema conforme può essere impiegato in un contesto diverso da quello previsto, gestito senza la necessaria verifica umana o concorrere a un danno per ragioni non esaurite dal controllo di conformità. D'altra parte, la sola prova di una non conformità non accerta automaticamente ogni elemento della responsabilità, salve le specifiche regole sull'esibizione e sulla presunzione causale. La direttiva (UE) 2024/2853, richiamata dagli artt. 16 e 19, dovrà essere recepita entro il 9 dicembre 2026 e riguarda i prodotti immessi sul mercato o messi in servizio dalla data prevista dalla fonte europea; alla data di questo scritto non si può trattare il suo futuro recepimento come un testo nazionale già verificato.²⁰

Un sistema di IA può essere parte di un prodotto, oppure il danno può dipendere soprattutto dal modo in cui qualcuno lo ha impiegato. I due percorsi non chiedono necessariamente la prova dei medesimi fatti: difetto, condotta, soggetto responsabile e data di immissione sul mercato assumono peso diverso secondo il titolo della domanda. L'art. 16, comma 3, preserva il coordinamento con la futura disciplina nazionale sui prodotti difettosi; alla data di questo capitolo quel testo non è ancora verificabile. Dopo aver facilitato l'accesso alla prova e delimitato la presunzione causale, il decreto considera un'ultima difficoltà pratica del danneggiato: sapere se esista una copertura assicurativa contro la quale agire direttamente.

10. Assicurazione, tempo della legge e responsabilità della decisione

L'art. 20 offre al danneggiato un ulteriore percorso, subordinato però all'esistenza di una copertura della responsabilità civile. Prima di agire, egli può chiedere al soggetto cui ritiene imputabile il danno se sia assicurato per quel rischio. La richiesta non costituisce condizione di procedibilità. Il destinatario comunica entro trenta giorni se esiste il contratto, i suoi estremi e l'impresa assicuratrice; la mancata o incompleta risposta può essere valutata dal giudice come argomento di prova ai sensi dell'art. 116 c.p.c. Nessuna parte della norma impone, per il solo utilizzo di un sistema di IA, la stipulazione di un'assicurazione. Il diritto all'informazione serve a rendere praticabile un'azione diretta quando una copertura vi sia.²¹

Il foro aggiuntivo previsto dall'art. 16, comma 4, risponde a un'esigenza affine di accesso alla tutela. Quando il danneggiato è una persona fisica che agisce per

20 D.lgs. n. 160 del 2026, artt. 18 e 19. Direttiva (UE) 2024/2853, art. 22, e scheda istituzionale sui termini di recepimento e applicazione: testo online.

21 D.lgs. n. 160 del 2026, art. 20, commi 1-6. La disposizione parla di contratto di assicurazione relativo al danno e non istituisce un obbligo generale di assicurazione.

scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta, è competente anche il giudice del luogo della sua residenza o del suo domicilio. La norma non modifica l'onere di provare i fatti della domanda, ma riduce un possibile ostacolo territoriale all'azione. Il suo ambito va letto secondo i requisiti espressi: non qualunque persona fisica beneficia del foro in ogni rapporto e la competenza aggiuntiva non trasforma il convenuto in un «professionista» secondo una qualificazione automatica. L'accesso al giudice, quello alla prova e quello a un eventuale assicuratore operano quindi su ostacoli diversi alla tutela.

L'azione diretta nei confronti dell'impresa è contenuta entro le somme assicurate. L'assicuratore può opporre al danneggiato le eccezioni contrattuali anteriori al sinistro; se paga, conserva la rivalsa verso l'assicurato nella misura in cui il contratto gli avrebbe consentito di rifiutare o ridurre la prestazione. Nel giudizio è litisconsorte necessario il soggetto individuato come responsabile del danno; la prescrizione dell'azione diretta coincide con quella dell'azione nei confronti di tale soggetto. Il modello processuale non separa quindi l'impresa dal fatto generatore della responsabilità: la presenza del presunto responsabile serve all'accertamento del fatto, del titolo e del danno anche quando la domanda sia rivolta direttamente all'assicuratore.

L'assicurazione rende meno gravoso, quando esiste e nei limiti del contratto, il conseguimento della riparazione. Non decide però chi sia responsabile del fatto; la presenza del presunto responsabile nel giudizio e la possibilità di rivalsa dell'assicuratore mostrano che il trasferimento economico del rischio non sostituisce la sua attribuzione giuridica. Il decreto conclude così il percorso civilistico nello stesso punto in cui lo aveva aperto: la tecnologia non elimina la necessità di ricostruire una condotta, un danno e il rapporto fra i due.

Rimane il tempo dell'attuazione. L'art. 21, comma 1, concede un anno dall'entrata in vigore per adeguare al capo II del titolo I i sistemi già contrattualizzati, in sviluppo, in sperimentazione o in uso per finalità di polizia. Il riferimento comprende gli artt. 3-6, non tutto il titolo I e, in particolare, non menziona il capo III sulle tecnologie biometriche. Il comma 2, per le disposizioni del titolo I la cui applicazione è prevista direttamente ovvero dipende dal regolamento europeo, prescrive l'osservanza dei termini di entrata in vigore e di compiuta attuazione di quest'ultimo. Vi sono dunque due regole temporali differenti: la prima riguarda l'adeguamento dei sistemi preesistenti alle disposizioni nazionali indicate; la seconda presuppone di verificare, norma per norma, il rapporto con il regolamento e il relativo calendario. Il rinvio alle fonti secondarie per alcuni requisiti tecnici non autorizza a considerare già emanati

provvedimenti che, alla data di questo capitolo, non risultano dal testo esaminato.

Le garanzie descritte richiedono una organizzazione capace di metterle in pratica. La clausola dell'art. 22, che impone alle amministrazioni di operare con le risorse disponibili e senza nuovi o maggiori oneri, non dimostra che la formazione, i log, le valutazioni d'impatto e il controllo qualificato siano privi di costi. Del pari, la dichiarazione degli artt. 1, comma 3, e 3, comma 7, di non introdurre nuovi obblighi rispetto al regolamento europeo non priva di effetto le modalità nazionali di autorizzazione e di uso. La loro concreta tenuta dovrà essere misurata sul funzionamento delle amministrazioni e sul coordinamento con le scadenze dell'Unione, senza confondere obblighi regolatori del sistema e condizioni poste all'attività di polizia.

Il bilancio del decreto dipenderà anche dalla qualità degli atti che produrrà. Il testo è più incisivo quando prescrive sequenze e conseguenze controllabili, come la delimitazione di una ricerca o la cancellazione dei risultati illeciti; è più esposto a una attuazione soltanto formale quando rinvia a requisiti tecnici futuri e a controlli affidati a strutture senza risorse aggiuntive. Un'autorizzazione che non spieghi il perimetro dell'operazione, una revisione umana di cui non resti traccia e un log inutilizzabile per ricostruire il confronto non realizzerebbero la stessa garanzia per il solo fatto di portarne il nome. È una valutazione sulla possibile applicazione della legge, non la constatazione di prassi già formate: alla data di questo capitolo tali prassi non sono ancora osservabili.

Si può ora tornare al passaggio dal quale siamo partiti. Il risultato prodotto da un sistema acquista rilievo giuridico soltanto entro un'attività umana determinata: qualcuno ha scelto il fine, composto la base dei dati, autorizzato l'uso, valutato l'output o omissis una cautela dovuta. Il decreto non riconduce tutte queste scelte a una unica regola di responsabilità; rende invece più visibili i punti in cui esse devono poter essere ricostruite. Quando una ricerca è contestata, occorre verificare la sua base e il percorso autorizzativo; quando un pericolo è imputato penalmente, la condotta e il dovere esigibile; quando un danno è allegato, il titolo della domanda e le prove accessibili. La difficoltà tecnica del sistema non può dispensare da queste verifiche, ma nemmeno autorizza ad anticiparne l'esito. È in questa possibilità di attribuire e discutere le scelte, più che nella sola presenza formale di un operatore, che si misura la portata delle garanzie introdotte dal decreto.

Lecture consigliate

- GALLI F., «Law Enforcement and Data-Driven Predictions at the National and EU Level: A Challenge to the Presumption of Innocence and Reasonable Suspicion?», in *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge, 2021, pp. 111-128.
- HILDEBRANDT M., *Law for Computer Scientists and Other Folk*, Oxford University Press, Oxford, 2020.
- MICKLITZ H.-W., POLLICINO O., REICHMAN A., SIMONCINI A., SARTOR G., DE GREGORIO G. (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge, 2021.
- PASQUALE F., *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge (Mass.), 2015.
- REICHMAN A., SARTOR G., «Algorithms and Regulation», in *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge, 2021, pp. 131-181.