

Prime osservazioni sugli schemi di Decreti Legislativi attuativi della Legge n. 132/2025 in materia di intelligenza artificiale

1. Premessa

L'avvento dell'intelligenza artificiale ha posto sfide inedite ai tradizionali modelli di regolazione, rendendo necessario un approccio innovativo, adeguato alla natura trasversale di dette tecnologie. La capacità dell'intelligenza artificiale di incidere simultaneamente su molteplici ambiti della vita sociale – dalla sanità alla giustizia, dal lavoro alla pubblica amministrazione – ha reso infatti indispensabile l'elaborazione di una disciplina capace di coniugare l'innovazione tecnologica, la tutela dei diritti fondamentali e il rispetto dei principi costituzionali¹.

In siffatto contesto, con decorrenza 1° agosto 2024 è (come noto) entrato in vigore il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 recante disposizioni armonizzate in materia di intelligenza artificiale con l'espresso fine di istituire un quadro giuridico uniforme per lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale nell'Unione Europea.

Il Regolamento, noto anche come “AI Act”, promuove quindi lo sviluppo e l'impiego di un'intelligenza artificiale antropocentrica, affidabile e sicura, al fine di tutelare la salute, la sicurezza, la democrazia, lo Stato di diritto, l'ambiente e i diritti sanciti dalla Carta dei diritti fondamentali dell'Unione europea. Al contempo, impone agli stati membri di astenersi dall'adottare discipline nazionali che introducano restrizioni autonome allo sviluppo e all'utilizzo dell'IA, al fine di evitare la frammentazione del mercato interno derivante da normative nazionali divergenti.

In specifico, dopo aver definito i propri obiettivi (Art. 1), il proprio ambito applicativo e le proprie principali definizioni (Artt. 2-3), il Regolamento ha classificato i sistemi di intelligenza artificiale in base al livello di rischio che essi presentano, distinguendo tra rischi inaccettabili, alti, limitati o minimi. L'AI Act ha così adottato un approccio basato sul rischio (*risk-based approach*), prevedendo un regime di obblighi differenziato in relazione al livello di rischio presentato dai sistemi di intelligenza artificiale in rilievo.

L'atto normativo europeo individua quattro categorie di sistemi di IA:

- la prima comprende i sistemi che presentano un rischio inaccettabile, il cui impiego è cioè ritenuto incompatibile con i valori e i diritti fondamentali dell'Unione europea e la cui immissione sul mercato, messa in servizio ed utilizzazione sono espressamente vietate (Capo II, art. 5).

¹ G. RICCIO, *L'Intelligenza Artificiale nel Quadro Normativo Italiano: Un'Analisi Comparativa della Legge 132/2025 nel Contesto Europeo e Internazionale*, in *Ratio Iuris*, 2026, p. 4.

- La seconda riguarda i sistemi di IA ad alto rischio, disciplinati al Capo III ed individuati secondo i criteri di classificazione stabiliti dall'art. 6 del Regolamento. Detti sistemi possono essere immessi sul mercato o messi in servizio solo previa verifica della loro conformità ai requisiti previsti dal Capo III, Sezione 2, attraverso una procedura di valutazione svolta dal fornitore oppure, nei casi previsti, da un organismo notificato indipendente (Art. 43).
- La terza categoria è costituita dai sistemi di IA soggetti ad obblighi di trasparenza (Capo IV). Per questi sistemi il Regolamento impone specifici obblighi informativi, prevedendo inoltre che le persone fisiche siano chiaramente informate quando interagiscano con un sistema di intelligenza artificiale o quando siano esposte a contenuti generati o manipolati artificialmente, nei casi previsti dall'art. 50.
- Infine, rientrano nell'ultima categoria i sistemi di IA a rischio minimo (Capo X). Per detti sistemi non sono previsti obblighi ulteriori rispetto a quelli derivanti dalla normativa settoriale applicabile e dalla disciplina generale dell'Unione europea, ferma restando la possibilità di aderire volontariamente ai codici di condotta promossi dal Regolamento.

Il Capo XII dell'AI Act disciplina poi il regime sanzionatorio. In particolare, con l'art. 99 si è demandato agli Stati membri il compito di definire le sanzioni e le altre misure di esecuzione applicabili alle violazioni del Regolamento nel rispetto dei principi di effettività, proporzionalità e dissuasività.

Nell'esercizio di siffatta competenza, gli Stati sono stati altresì chiamati a tener conto degli orientamenti della Commissione europea e della sostenibilità economica delle PMI, comprese le start-up.

2. Le misure nazionali di adeguamento al Regolamento (UE) 2024/1689

2.1. La Legge delega n. 132 del 2025

A valle dell'entrata in vigore dell'AI Act, il 23 settembre 2025 l'Italia ha dunque promulgato la Legge delega n. 132, recante «*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*», divenendo il primo Stato membro dell'Unione europea a dotarsi di una disciplina organica di adeguamento al Regolamento (UE) 2024/1689.

In specifico, la Legge n. 132/2025 è intervenuta direttamente in alcuni settori strategici, quali la sanità (Art. 7), il lavoro (Art. 11), la Pubblica amministrazione (Art. 14) e la giustizia (Art. 15), stabilendo e fissando principi generali per la ricerca, sperimentazione, sviluppo, adozione e utilizzo dei sistemi e dei modelli di intelligenza artificiale.

Siffatta Legge non si è tuttavia limitata a disciplinare gli aspetti rimessi alla competenza degli Stati membri dal Regolamento (UE) 2024/1689, ma ha introdotto (da un lato) una nuova fattispecie penale e (dall'altro) delegato al Governo l'adozione di ulteriori norme volte a coniugare le esigenze di armonizzazione perseguite dall'AI Act con i principi dell'ordinamento costituzionale italiano.

Quanto alla novella penale, il Legislatore ha introdotto la previsione del nuovo art. 612-*quater* c.p., rubricato «*illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*», con l'obiettivo di contrastare il fenomeno della diffusione illecita di immagini generate o alterate mediante sistemi di intelligenza artificiale.

La disposizione punisce, con la reclusione da uno a cinque anni, la condotta di chi diffonde, pubblica o cede, senza il consenso dell'interessato, immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale, qualora siano idonei a trarre in inganno circa la loro autenticità e a cagionare un danno ingiusto alla persona offesa.

La nuova fattispecie è pertanto volta a contrastare la realizzazione e la diffusione dei c.d. *deepfake*, ossia contenuti multimediali generati o manipolati mediante sistemi di intelligenza artificiale idonei a riprodurre in modo ingannevole persone, oggetti o luoghi reali. La collocazione dell'art. 612-*quater* c.p. tra i delitti contro la libertà individuale evidenzia la volontà del Legislatore di tutelare, in via principale, la dignità e la libertà morale della persona, messe a rischio dalla diffusione di tali contenuti².

Quanto alla delega:

- con l'art. 16 della Legge 132 si è delegato il Governo ad adottare una disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale e con
- il successivo art. 24 si è delegato il Governo ad adeguare la normativa italiana all'AI Act, ad attribuire poteri alle autorità nazionali, a disciplinare vigilanza e sanzioni, ad introdurre percorsi di formazione e alfabetizzazione sull'IA, a regolamentare l'uso dell'IA nell'attività di polizia, a rafforzare ricerca e trasferimento tecnologico, a definire i poteri ispettivi, ad adeguare il sistema sanzionatorio, nonché a disciplinare i casi di realizzazione e impiego illeciti dei sistemi di IA, introducendo nuove fattispecie di reato, regole sulla responsabilità civile e penale, misure cautelari e la disciplina dell'uso dell'IA nelle indagini preliminari.

² Cfr. A MILONE, *Il diritto penale alla prova dell'intelligenza artificiale: alcune riflessioni intorno all'art. 612-*quater* c.p.*, in *Giurisprudenza Penale Web*, 2026, p. 6.

In attuazione dei predetti articoli 16 e 24, nella seduta del Consiglio dei Ministri in data 10 giugno 2026, il Governo ha quindi emesso i due schemi di Decreti Legislativi delegati commentati di seguito che – secondo il Comunicato Stampa del Consiglio dei Ministri n. 177/2026 – risultano «coerenti e conformi» al Regolamento europeo e che «non introducono una disciplina alternativa rispetto al quadro europeo, ma ne assicurano l’attuazione nell’ordinamento nazionale»³.

2.2. Il primo schema di Decreto Legislativo

Il primo schema di Decreto Legislativo ha ad oggetto i poteri delle autorità nazionali e la formazione in materia di intelligenza artificiale, mirando ad attuare le deleghe contenute nell’art. 24, co. 1 e 2, lett. a), b), c), d), e), f), g), i), l), m) e n) della Legge Delega 132/2025.

Dopo un primo Capo composto da un unico articolo dedicato alle definizioni, il Capo II disciplina i «*poteri delle Autorità nazionali per l’intelligenza artificiale*». In particolare, il Decreto individua quali autorità di riferimento l’Agenzia per la cybersicurezza nazionale (ACN) e l’Agenzia per l’Italia digitale (AgID), riservando specifiche competenze settoriali alla Banca d’Italia, alla CONSOB, all’IVASS e al Garante per la protezione dei dati personali.

Una volta delineate le attribuzioni delle autorità competenti, lo stesso Decreto disciplina i meccanismi di coordinamento e di cooperazione tra le stesse, prevedendo la possibilità di ricorrere ad accordi e protocolli d’intesa al fine di assicurare uno scambio tempestivo e completo di dati ed informazioni necessari allo svolgimento delle rispettive funzioni.

Di particolare rilievo è la quinta Sezione del Capo II, dedicata alle «*disposizioni sanzionatorie*». Anzitutto, all’art. 19, co. 1, si statuisce che «*l’Autorità nazionale di notifica e le Autorità nazionali di vigilanza del mercato adottano tutte le misure necessarie per garantire un’attuazione corretta ed efficace del presente capo, tenendo in considerazione, in particolare, quanto previsto dall’articolo 99 del regolamento IA*», precisando, poi, al secondo comma, che «*ai fini dell’attuazione dell’articolo 99, paragrafo 1, del regolamento IA, nell’ambito dell’esercizio dei poteri sanzionatori previsti dal presente capo sono inclusi gli avvertimenti e le misure non pecuniarie di cui all’articolo 22 del presente decreto, applicabili in caso di violazione del regolamento IA*».

Il sistema sanzionatorio delineato dagli artt. 20–23 dello schema di Decreto attribuisce, dunque, competenze differenziate tra AgID, Autorità nazionali di vigilanza del mercato e Autorità nazionale di notifica, secondo una logica per ambiti di intervento e tipologia di misura.

³ Cfr. Comunicato stampa del Consiglio dei ministri n. 177.

In primo luogo, l'Agenzia per l'Italia Digitale (AgID), nell'esercizio delle funzioni di autorità di notifica, è competente a irrogare esclusivamente le sanzioni amministrative pecuniarie previste dall'art. 99, par. 4, lett. f), e par. 5 del AI Act⁴ (Art. 20). Si tratta perciò di un potere sanzionatorio di natura esclusivamente pecuniaria, collegato allo svolgimento delle attività di notifica e vigilanza sugli operatori coinvolti.

Le Autorità nazionali di vigilanza del mercato sono a propria volta titolari del potere di irrogare le sanzioni previste dal Capo II nei confronti dei soggetti individuati dall'art. 99, par 1 del Regolamento europeo. In questo ambito, dette Autorità possono irrogare sia sanzioni pecuniarie, disciplinate dall'art. 23, sia, per le violazioni «*caratterizzate da scarsa offensività o pericolosità e in linea con i criteri richiamati all'articolo 23, comma 12*»⁵, misure alternative di carattere non pecuniario.

Queste ultime si sostanziano (da un lato) nell'ordine di rimuovere la violazione e di non reiterarla, con eventuale indicazione delle misure da adottare e del relativo termine di attuazione; (dall'altro) qualora l'illecito risulti già cessato, nella pubblicazione di una dichiarazione di accertamento della violazione e di individuazione del soggetto responsabile.

Si tratta quindi di misure alternative alla sanzione pecuniaria, applicabili in presenza di violazioni caratterizzate da scarsa offensività o pericolosità. Resta tuttavia fermo che, in caso di inottemperanza all'ordine di cessazione, l'Autorità possa procedere all'irrogazione delle sanzioni pecuniarie previste dall'art. 23, con un aumento fino a un terzo rispetto alla sanzione originariamente applicabile, nei limiti dei massimali stabiliti.

A questo riguardo, l'art. 23 disciplina in modo analitico il sistema delle sanzioni amministrative pecuniarie, prevedendo importi differenziati in base alla gravità della violazione e agli obblighi violati dall'AI Act: le sanzioni sono calibrate in termini assoluti o percentuali sul fatturato mondiale annuo del soggetto responsabile e possono essere ridotte del 50% nel caso in cui l'autore sia una persona fisica.

⁴ Cfr. art. 99, paragrafo 4, lett. f) e paragrafo 5 del Regolamento (UE) 2024/1689, ove si afferma che «*la non conformità a qualsiasi delle seguenti disposizioni connesse a operatori o organismi notificati, diverse da quelle di cui all'articolo 5, è soggetta a sanzioni amministrative pecuniarie fino a 15 000 000 EUR o, se l'autore del reato è un'impresa, fino al 3 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore i requisiti e gli obblighi degli organismi notificati a norma dell'articolo 31, dell'articolo 33, paragrafi 1, 3 e 4, o dell'articolo 34*» e che «*la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti per dare seguito a una richiesta è soggetta a sanzioni amministrative pecuniarie fino a 7 500 000 EUR o, se l'autore del reato è un'impresa, fino all'1 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore*».

⁵ Art. 22 della bozza del Decreto legislativo.

Nella determinazione dell'importo, le Autorità competenti applicano i criteri stabiliti dal Regolamento europeo, tenendo conto della natura della violazione e della condizione soggettiva del trasgressore, con particolare attenzione alle PMI, microimprese e start-up innovative, per le quali trovano applicazione criteri di attenuazione specifici.

Si tratta di sanzioni che hanno una natura formalmente amministrativa (si veda, ad esempio, lo stesso articolo 23, che si apre con la formula «*salvo che il fatto costituisca reato*»), ma sostanzialmente afflittiva e, come tali, riconducibili alla nozione sostanziale ed autonoma di “materia penale” elaborata dalla CEDU secondo i criteri *Engel*⁶, atteso (in specifico) che (i) la finalità di dette sanzioni è punitiva e/o deterrente; (ii) sono di importo elevato e (iii) incidono significativamente sulla sfera economica del soggetto sanzionato.

La severità del regime sanzionatorio delineato dall'AI Act emerge con particolare evidenza dal confronto con il GDPR (*General Data Protection Regulation* - Regolamento UE 2016/679). Il legislatore europeo – e, quindi, quello italiano, posto che il Decreto legislativo richiama il Regolamento UE sull'intelligenza artificiale – ha infatti previsto soglie sanzionatorie più elevate rispetto a quelle stabilite dal Regolamento in materia di protezione dei dati personali, evidenziando così la volontà di attribuire particolare rilevanza ai rischi connessi all'impiego dei sistemi di intelligenza artificiale. Ne consegue un rafforzamento dell'apparato repressivo, destinato ad incidere in misura significativa sugli operatori economici che non rispettino gli obblighi imposti dal Regolamento.

Il Capo III dello schema di Decreto viene pertanto dedicato alla formazione in materia di intelligenza artificiale, prevedendosi l'attivazione di percorsi di alfabetizzazione rivolti a studenti, docenti, professionisti, pubbliche amministrazioni e magistrati.

Con specifico riferimento a questi ultimi, l'atto normativo attribuisce alla Scuola superiore di magistratura il compito di promuovere percorsi formativi dedicati all'intelligenza artificiale, articolati, ex art. 46 co. 1, lungo tre principali direttrici:

- a) la formazione sui profili tecnici connessi al funzionamento ed ai limiti dei sistemi di intelligenza artificiale impiegati nell'attività giudiziaria e nell'organizzazione dei servizi relativi alla giustizia.
- b) la formazione sui profili giuridici relativi alla disciplina dell'intelligenza artificiale.
- c) la formazione relativa all'impatto dell'impiego dei sistemi di intelligenza artificiale sull'organizzazione giudiziaria e sulla tutela dei diritti delle persone.

Di particolare rilievo è anche la previsione dell'art. 43 che disciplina l'intelligenza artificiale con riferimento alla salute e sicurezza nei luoghi di lavoro. In specifico i sistemi

⁶ Corte EDU, *Engel and Others v. Netherlands*, 8 giugno 1976.

di intelligenza artificiale che incidono sull'organizzazione del lavoro o sui ritmi produttivi devono essere inclusi nella valutazione dei rischi prevista dal D.lgs. 9 aprile 2008, n. 81. Le aziende sono pertanto chiamate ad adottare un approccio integrato alla *governance* dell'IA, coordinando gli aspetti giuslavoristici, di tutela della *privacy* e di salute e sicurezza sul lavoro.

Infine, i Capi IV e V Capo dello schema di Decreto sono dedicati (rispettivamente) alle informazioni aziendali ed alle esperienze tecnico-industriali concernenti dati, algoritmi e metodi matematici; nonché, alle disposizioni finanziarie.

2.3. Il secondo schema di Decreto Legislativo

Il secondo schema di Decreto legislativo assume particolare rilievo sotto il profilo penalistico e processual-penalistico e mira ad attuare le deleghe contenute nell'art. 24, co. 1, co. 2, lett. h, co. 3 e co. 5 della L. n. 132 del 2025.

Segnatamente, il Titolo I del Decreto disciplina l'impiego dei sistemi di intelligenza artificiale da parte degli organi, uffici e comandi delle Forze di Polizia. Dopo un articolo introduttivo dedicato alle definizioni rilevanti in materia (Art. 2), il Capo III reca la specifica disciplina concernente la ricerca, lo sviluppo, l'addestramento, la formazione, la sperimentazione e l'utilizzo dei sistemi di intelligenza artificiale nell'esercizio delle attività di Polizia.

Particolare rilievo assume, anzitutto, l'art. 3, che enuncia i principi generali in materia di ricerca, sperimentazione, sviluppo, addestramento, convalida e utilizzo dei sistemi e dei modelli di intelligenza artificiale destinati alle attività di Polizia. In linea con l'approccio antropocentrico che permea l'AI Act e con il principio della sorveglianza umana di cui all'art. 14 del Regolamento, la disposizione stabilisce che tali sistemi possano essere impiegati esclusivamente quale strumento di supporto all'attività di Polizia (co. 3). Inoltre che l'utilizzo degli *output* generati dai sistemi di intelligenza artificiale sia sempre preceduto da un'adeguata revisione umana qualificata, da documentare in modo tale da assicurarne la tracciabilità (co. 4)⁷.

L'art. 6 prevede poi l'attivazione da parte delle Forze di Polizia di corsi di formazione in materia di intelligenza artificiale applicata alle attività di Polizia che debbono assicurare la comprensione dei principi di funzionamento e le potenzialità dei sistemi di intelligenza artificiale, la «*conoscenza dei limiti, dei bias e degli errori dei sistemi di intelligenza artificiale*», nonché la capacità di interpretazione critica degli output e la consapevolezza

⁷ Cfr. B. FRAGASSO, *Disposizioni attuative in materia di intelligenza artificiale: il reato di omessa adozione di misure di sicurezza nei sistemi di I.A. e altre novità in materia di autorità di vigilanza, identificazione biometrica, responsabilità da reato degli enti e responsabilità civile*, in *Sistema Penale*, 12 giugno 2026, p. 4.

delle implicazioni giuridiche e dei rischi di cybersicurezza connessi all'utilizzo dei sistemi di intelligenza artificiale.

Il Capo III assume particolare rilievo anche perché reca la disciplina relativa ai «*sistemi di intelligenza artificiale utilizzati nelle attività di polizia per l'etichettatura, il filtraggio e la categorizzazione di dati biometrici, per l'identificazione biometrica remota in tempo reale per finalità di prevenzione o di protezione e per il riconoscimento facciale a posteriori a fini di contrasto dei reati*».

L'art. 8 disciplina l'impiego, da parte delle Forze di Polizia, dei sistemi di identificazione biometrica remota in tempo reale, ammettendone l'utilizzo esclusivamente nelle ipotesi consentite dall'art. 5, par. 1, lett. h), punti i) e ii), dell'AI Act⁸ (co.1). La disposizione circoscrive poi ulteriormente il ricorso a siffatte tecnologie, prevedendo che esse possano essere impiegate solo per confermare l'identità delle persone specificamente interessate, oppure per la ricerca mirata, anche dinamica e comprensiva della localizzazione, di persone specificatamente individuate o individuabili in relazione alla minaccia da prevenire o all'attività di ricerca da svolgere (co. 2). L'utilizzo è subordinato all'impiego di banche dati lecitamente costituite (co. 3), con espresso divieto di ricorrere a banche dati alimentate (anche solo in parte) mediante tecniche di *scraping* non mirato⁹ o comunque formate in violazione della disciplina vigente in materia di protezione dei dati personali.

L'art. 8 introduce inoltre una specifica garanzia procedimentale, subordinando l'impiego dei sistemi di identificazione biometrica remota in tempo reale da parte delle forze di polizia alla preventiva autorizzazione del Procuratore della Repubblica presso il Tribunale del capoluogo del distretto nel quale sono emerse le esigenze di prevenzione o di ricerca (co. 4). Si prevede, ancora, che «*l'autorizzazione deve essere concessa con riguardo a uno specifico evento o per il tempo strettamente necessario, in ogni caso non superiore a quindici giorni, prorogabili dal procuratore della Repubblica, con decreto motivato per periodi successivi di quindici giorni qualora permangano le condizioni di cui al comma 1, nonché con riferimento ad una area territoriale delimitata e alla indicazione delle persone specificamente interessate e ricercate. La medesima*

⁸ Cfr. art. 5, par. 1, lett. h), punti i) e ii) ove si afferma che «*sono vietate le pratiche di IA seguenti: [...] l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti: i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico*».

⁹ Ai sensi dell'art. 2, co. 1, lett. k), dello schema di Decreto legislativo, per *scraping* non mirato si intende «*l'estrazione e la raccolta automatizzata e indiscriminata, su larga scala, mediante l'utilizzo di un sistema di intelligenza artificiale, di immagini facciali dalla rete internet o da filmati di telecamere a circuito chiuso, allo scopo di creare o ampliare banche dati di riconoscimento facciale*».

autorizzazione può essere concessa, altresì, soltanto previa effettuazione delle valutazioni di cui all'articolo 5, paragrafo 2, del regolamento IA» (co. 5).

Infine, nei casi di urgenza, è previsto che, ove il ritardo possa cagionare un pregiudizio grave e irreparabile per le finalità indicate dal comma 1, l'utilizzo del sistema possa essere avviato dall'organo di Polizia procedente, previa comunicazione, anche orale, al P.M. (co. 6). L'autorità è tenuta in ogni caso a trasmettere il provvedimento al Pubblico Ministero senza ritardo e, comunque, entro dodici ore dall'avvio dell'operazione; il Pubblico Ministero, qualora ritenga sussistenti i presupposti previsti dalla legge, è tenuto a propria volta a provvedere nelle successive dodici ore (co. 7). Si prevede, inoltre, l'inutilizzabilità degli elementi acquisiti in caso di inosservanza dei suddetti requisiti (co. 8).

Il successivo articolo 10 disciplina poi il riconoscimento facciale a posteriori mediante sistemi di videosorveglianza integrati con componenti di intelligenza artificiale, prevedendo che tali tecnologie possano essere attivate solo dopo la realizzazione di un fatto di reato, anche tentato, e solo per l'identificazione di persone già indiziate.

Tanto chiarito, ai fini della presente analisi, assume rilievo senz'altro preminente il Titolo II dello schema di Decreto, specificamente dedicato alle *«disposizioni penali, sostanziali e processuali, in materia di realizzazione e impiego illeciti dei sistemi di intelligenza artificiale e disposizioni processuali civili in materia di risarcimento dei danni cagionati dall'utilizzo dei medesimi sistemi»*.

In via segnata, il Capo I del Titolo II dà attuazione alla delega conferita dall'art. 24, comma 3, della Legge n. 132 del 2025, nel rispetto dei principi e criteri direttivi previsti dal comma 5. In particolare, esso prevede l'introduzione di autonome fattispecie di reato fondate sull'omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale; disciplina l'impiego di tali sistemi nell'ambito delle indagini preliminari; introduce strumenti, anche di natura cautelare, volti alla rimozione dei contenuti illecitamente generati, con specifico riferimento al sequestro preventivo e reca, infine, le necessarie disposizioni di coordinamento.

Principiando dal Capo I vi è allora che, con l'art. 12 del Decreto, si introduce la nuova fattispecie penale di *«omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi»* disciplinata dal neo introdotto art. 437-bis del Codice penale.

Siffatta nuova disposizione prevede testualmente, al primo comma, che *«chiunque omette di adottare le misure tecniche di sicurezza, previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato o l'utilizzo professionale di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi ovvero omette di adottare misure di sorveglianza umana è*

punito con la reclusione da uno a cinque anni, quando da tali omissioni derivi pericolo concreto per la vita o l'incolumità pubblica o individuale. Qualora dal fatto derivi un pericolo concreto per l'incolumità pubblica o per la sicurezza dello Stato, la pena è della reclusione da due a otto anni”.

Il successivo secondo comma dispone quindi a propria volta che *“salvo che il fatto costituisca più grave reato, chiunque, al di fuori dei casi indicati al primo comma, altera sistemi di intelligenza artificiale ad alto rischio è punito, qualora dal fatto derivi un pericolo concreto per la vita o l'incolumità individuale, con la reclusione da due a sei anni. Qualora dal fatto derivi un pericolo concreto per l'incolumità pubblica o per la sicurezza dello Stato, la pena è della reclusione da tre a dieci anni”.*

La previsione si chiude con un terzo comma a tenore del quale *“se taluno dei fatti previsti dal comma primo è commesso per colpa grave, la pena è ridotta da un terzo a un sesto».*

Bene allora chiarire (innanzitutto) che, sebbene l'utilizzo della formula «chiunque» possa, a una prima lettura, indurre a qualificare la fattispecie come reato comune, un esame sistematico conduce ad una conclusione diversa.

Tanto il Regolamento UE 2024/1689, quanto il Decreto legislativo di attuazione individuano invero uno specifico ambito soggettivo di applicazione degli obblighi di sicurezza; coerentemente, il nuovo articolo 437-bis c.p. presuppone che il dovere di adottare le misure tecniche di sicurezza e di sorveglianza umana gravi esclusivamente sui soggetti che progettano, addestrano, producono, immettono sul mercato ovvero utilizzano professionalmente sistemi di intelligenza artificiale ad alto rischio. Ne consegue che la fattispecie, pur formulata in termini apparentemente generali, presenti la struttura di un reato proprio.

Sotto il profilo oggettivo, è chiaro come ci si trovi di fronte ad un reato omissivo proprio, in quanto la condotta tipica consiste nell'omessa adozione delle misure tecniche di sicurezza o di sorveglianza umana prescritte dalla disciplina di settore. La punibilità, tuttavia, non consegue alla mera inosservanza dell'obbligo, ma richiede che da detta omissione derivi un pericolo concreto, essendo demandato al Giudice l'accertamento dell'effettiva idoneità della condotta omissiva a determinare una situazione di pericolo, non essendo invero sufficiente la semplice violazione delle prescrizioni cautelari.

Quanto al regime sanzionatorio, il secondo periodo del primo comma introduce una circostanza aggravante speciale, prevedendo che la pena della reclusione da uno a cinque anni sia aumentata da due a otto nel caso in cui dall'omissione derivi un pericolo concreto per l'incolumità pubblica o per la sicurezza dello Stato. Di contro, il comma secondo configura una fattispecie autonoma di reato, atteso che descrive una diversa condotta

(alterazione dei sistemi di intelligenza artificiale) e prevede una propria cornice edittale (due-sei anni di reclusione).

Infine, il terzo comma introduce una responsabilità più mite nell'ipotesi in cui il reato sia condotto, testualmente, per “*colpa grave*”. In proposito, nella Relazione Illustrativa al Decreto si legge che *«la selezione della colpa grave come elemento di tipicità risponde a un'esigenza di proporzionalità: si circoscrive la punibilità alle macroscopiche violazioni delle regole di diligenza, evitando la criminalizzazione di ogni scostamento dallo standard tecnico in un dominio caratterizzato da rapida evoluzione e da una compresenza di standard tecnici nazionali, unionali e internazionali. In questi casi la pena è ridotta da un terzo a un sesto»*¹⁰.

Come anticipato, le modifiche non hanno interessato soltanto il Codice penale, ma anche il Codice di procedura penale. In particolare, l'art. 13 della bozza di Decreto legislativo interviene su quest'ultimo introducendo il nuovo art. 359-ter, rubricato *«identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale»*.

La sua collocazione nel Titolo IV del Libro dedicato alle attività del Pubblico Ministero conferma la funzione dello strumento di intelligenza artificiale quale mezzo di ricerca della prova nelle indagini preliminari. La nuova disposizione disciplina infatti i presupposti, le finalità e le modalità di impiego dei sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale nell'ambito del procedimento penale. Segnatamente, se ne consente l'utilizzo per confermare l'identità o localizzare persone gravemente indiziate della commissione dei reati indicati nell'allegato II del Regolamento (UE) 2024/1689, nonché per la ricerca di latitanti e di specifiche vittime di sottrazione, tratta o sfruttamento sessuale di esseri umani. Il confronto biometrico deve avvenire esclusivamente mediante banche dati di riferimento costituite da dati acquisiti lecitamente nel corso delle indagini o comunque accessibili all'autorità giudiziaria e alla polizia giudiziaria.

L'impiego del sistema è subordinato all'autorizzazione del Giudice per le indagini preliminari, su richiesta del Pubblico Ministero, con decreto motivato che delimita l'ambito territoriale, individua i soggetti interessati e stabilisce una durata massima di quindici giorni, prorogabile ove ne ricorrano i presupposti.

La norma codicistica disciplina inoltre una procedura d'urgenza che consente, in presenza di particolari esigenze, l'attivazione del sistema di intelligenza artificiale da parte del Pubblico Ministero e, nei casi eccezionali, della polizia giudiziaria, prevedendo il successivo controllo del Giudice. Infine, è sancita l'inutilizzabilità dei risultati ottenuti al

¹⁰ Cfr. relazione illustrativa allo schema del secondo Decreto legislativo attuativo della L. n. 132/2025.

di fuori dei casi consentiti dalla legge o in violazione delle garanzie procedurali previste, con conseguente cancellazione dei dati acquisiti, salvo che costituiscano corpo del reato.

La bozza di Decreto interessa anche il D.lgs. 8 giugno 2001, n. 231. L'articolo 15 dello schema di Decreto, rubricato «*modifiche al decreto legislativo 8 giugno 2001, n. 231*», introduce infatti l'art. 25-*vicies* (*reati commessi con l'uso di sistemi di intelligenza artificiale*), prevedendo che, in caso di commissione del delitto di cui all'art. 437-*bis* c.p., all'ente si applichi una sanzione pecuniaria da seicento a mille quote. Per il delitto previsto dall'art. 612-*quater* c.p. è stabilita invece una sanzione pecuniaria da duecento a settecento quote. In entrambe le ipotesi trovano inoltre applicazione le sanzioni interdittive previste dall'art. 9, comma 2, lett. b), c), d) ed e), del d.lgs. n. 231/2001.

Il successivo Capo II, intitolato «*strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di intelligenza artificiale*» dà infine attuazione alla delega prevista dall'art. 24, commi 3 e 5, lett. d), della Legge 23 settembre 2025, n. 132, con cui il Governo è stato delegato ad adottare uno o più decreti legislativi volti a disciplinare gli strumenti di tutela del danneggiato nei casi di responsabilità civile derivante dall'impiego di sistemi di intelligenza artificiale.

Detto Capo si apre con l'articolo 16 che individua l'ambito di applicazione delle nuove disposizioni. In specifico, si stabilisce che l'articolo 17, rubricato «*accesso alle prove*», si applichi a tutte le azioni di risarcimento, contrattuali ed extracontrattuali, per i danni causati dall'utilizzo di sistemi di intelligenza artificiale. Gli articoli 18 e 19 trovano invece applicazione solo quando il danno sia conseguenza della violazione di uno o più obblighi previsti dall'AI Act.

Segnatamente, gli articoli da 17 a 20 introducono specifici strumenti processuali volti a garantire una maggiore effettività della tutela risarcitoria: l'accesso alle prove relative al funzionamento del sistema di IA; la presunzione, salvo prova contraria, del nesso di causalità in caso di violazione dell'AI Act; la precisazione che la conformità al regolamento europeo non esclude la responsabilità e, da ultimo, l'azione diretta nei confronti dell'impresa di assicurazione del responsabile.

3. Note finali

L'impiego dell'intelligenza artificiale investe anche il processo penale e le garanzie dell'equo processo. Sul tema si è pronunciata la Corte europea dei diritti dell'uomo che ha evidenziato come l'impiego delle nuove tecnologie nel processo penale debba essere sempre rispettoso delle garanzie del giusto processo. In particolare, la Corte ha ribadito la necessità di assicurare il pieno esercizio del contraddittorio, la possibilità di contestare efficacemente le prove elettroniche, il rispetto del principio di immediatezza e, più in

generale, il diritto dell'imputato a essere giudicato da un tribunale umano, indipendente e imparziale¹¹.

L'esigenza di coniugare l'innovazione tecnologica con la tutela dei diritti fondamentali, emersa anche nella giurisprudenza della Corte EDU, trova dunque oggi espressione nel quadro normativo europeo e nazionale. La disciplina delineata dal Regolamento (UE) 2024/1689, dalla L. n. 132/2025 e dalle bozze dei due decreti legislativi evidenzia invero chiaramente la volontà del Legislatore (europeo e nazionale) di costruire un sistema organico di regolamentazione dell'intelligenza artificiale che sia volto a creare un equilibrio tra innovazione tecnologica, tutela dei diritti fondamentali ed esigenze di sicurezza.

In siffatto complesso contesto, il diritto penale è (e sarà) perciò chiamato senz'altro a confrontarsi con fenomeni tecnologici multiformi ed in continua evoluzione, che impongono (ed imporranno ancor più in futuro) un costante bilanciamento tra efficacia dell'intervento repressivo, principio di legalità e garanzie individuali. In specifico, come ammonito dalla Corte EDU, l'utilizzo di sistemi IT molto potenti non potrà mai tradursi in un affievolimento delle garanzie sostanziali e processuali proprie del diritto penale, ma dovrà essere passo-passo accompagnato da un quadro normativo capace di assicurare il rispetto dei principi di legalità, del diritto di difesa, del giusto processo e, più in generale, della dignità della persona.

¹¹ Cfr. D. CARDAMONE, *L'uso dell'intelligenza artificiale e la protezione di diritti fondamentali. Giurisprudenza della Corte Edu e giusto processo digitale*, in *Questione Giustizia*, 2026, pp. 6-8.