

SP

SISTEMA
PENALE

FASCICOLO

10/2025

COMITATO EDITORIALE Giuseppe Amarelli, Roberto Bartoli, Hervè Belluta, Michele Caianiello, Massimo Ceresa-Gastaldo, Adolfo Ceretti, Cristiano Cupelli, Francesco D'Alessandro, Angela Della Bella, Gian Paolo Demuro, Emilio Dolcini, Novella Galantini, Mitja Gialuz, Glauco Giostra, Antonio Gullo, Stefano Manacorda, Vittorio Manes, Luca Masera, Anna Maria Maugeri, Melissa Miedico, Vincenzo Mongillo, Francesco Mucciarelli, Claudia Pecorella, Marco Pelissero, Lucia Riscato, Marco Scoletta, Carlo Sotis, Costantino Visconti.

COMITATO SCIENTIFICO (REVISORI) Andrea Abbagnano Trione, Alberto Alessandri, Silvia Allegrezza, Chiara Amalfitano, Enrico Mario Ambrosetti, Ennio Amodio, Gastone Andrezza, Ercole Aprile, Giuliano Balbi, Marta Bargis, Enrico Basile, Fabio Basile, Alessandra Bassi, Teresa Bene, Carlo Benussi, Alessandro Bernardi, Marta Bertolino, Francesca Biondi, Rocco Blaiotta, Manfredi Bontempelli, Carlo Bonzano, Matilde Brancaccio, Carlo Bray, Renato Bricchetti, David Brunelli, Carlo Brusco, Silvia Buzzelli, Alberto Cadoppi, Lucio Camaldo, Gaia Caneschi, Stefano Canestrari, Giovanni Canzio, Francesco Caprioli, Matteo Caputo, Fabio Salvatore Cassibba, Donato Castronuovo, Elena Maria Catalano, Mauro Catenacci, Antonio Cavaliere, Francesco Centonze, Federico Consulich, Carlotta Conti, Stefano Corbetta, Roberto Cornelli, Fabrizio D'Arcangelo, Marcello Daniele, Gaetano De Amicis, Cristina De Maglie, Alberto De Vita, Jacopo Della Torre, Ombretta Di Giovine, Gabriella Di Paolo, Giandomenico Dodaro, Massimo Donini, Salvatore Dovere, Tomaso Emilio Epidendio, Luciano Eusebi, Riccardo Ferrante, Giovanni Fiandaca, Giorgio Fidelbo, Stefano Finocchiaro, Carlo Fiorio, Roberto Flor, Luigi Foffani, Désirée Fondaroli, Gabriele Fornasari, Gabrio Forti, Piero Gaeta, Alessandra Galluccio, Marco Gambardella, Alberto Gargani, Loredana Garlati, Giovanni Grasso, Giulio Illuminati, Gaetano Insolera, Roberto E. Kostoris, Giorgio Lattanzi, Sergio Lorusso, Ernesto Lupo, Raffaello Magi, Vincenzo Maiello, Adelmo Manna, Grazia Mannozi, Marco Mantovani, Luca Marafioti, Enrico Marzaduri, Maria Novella Masullo, Oliviero Mazza, Francesco Mazzacuva, Claudia Mazzucato, Alessandro Melchionda, Chantal Meloni, Vincenzo Militello, Andrea Montagni, Gaetana Morgante, Lorenzo Natali, Renzo Orlandi, Luigi Orsi, Francesco Palazzo, Carlo Enrico Paliero, Lucia Parlato, Annamaria Peccioli, Chiara Perini, Lorenzo Picotti, Carlo Piergallini, Paolo Pisa, Luca Pistorelli, Daniele Piva, Oreste Pollicino, Domenico Pulitanò, Serena Quattrocchio, Tommaso Rafaraci, Paolo Renon, Maurizio Romanelli, Bartolomeo Romano, Gioacchino Romeo, Alessandra Rossi, Carlo Ruga Riva, Francesca Ruggieri, Elisa Scaroina, Laura Scomparin, Nicola Selvaggi, Sergio Seminara, Paola Severino, Rosaria Sicurella, Piero Silvestri, Fabrizio Siracusano, Nicola Triggiani, Andrea Francesco Tripodi, Giulio Ubertis, Maria Chiara Ubiali, Antonio Vallini, Gianluca Varraso, Vito Velluzzi, Paolo Veneziani, Francesco Viganò, Daniela Vigoni, Francesco Zacchè, Stefano Zirulia.

REDAZIONE Francesco Lazzeri, Giulia Mentasti (coordinatori), Dario Albanese, Enrico Andolfatto, Silvia Bernardi, Patrizia Brambilla, Pietro Chiaraviglio, Beatrice Fragasso, Elisa Grisonich, Alessandro Malacarne, Cecilia Pagella, Emmanuele Penco, Gabriele Pontepino, Sara Prandi, Tommaso Trinchera.

Sistema penale (SP) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.

La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.

La *Rivista* si uniforma agli standard internazionali definiti dal *Committee on Publication Ethics* (COPE) e fa proprie le relative linee guida.

I materiali pubblicati su *Sistema Penale* sono oggetto di licenza CC BY-NC-ND 4.00 International. Il lettore può riprodurli e condividerli, in tutto o in parte, con ogni mezzo di comunicazione e segnalazione anche tramite collegamento ipertestuale, con qualsiasi mezzo, supporto e formato, per qualsiasi scopo lecito e non commerciale, conservando l'indicazione del nome dell'autore, del titolo del contributo, della fonte, del logo e del formato grafico originale (salve le modifiche tecnicamente indispensabili). La licenza è consultabile su <https://creativecommons.org/licenses/by-nc-nd/4.0/>.

Peer review I contributi che la direzione ritiene di destinare alla sezione "Articoli" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "Altri contributi" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.

Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2023, p. 5 ss.

PROFILI PENALISTICI DELLA LEGGE SULL'INTELLIGENZA ARTIFICIALE: OSSERVAZIONI A PRIMA LETTURA

Legge 23 settembre 2025, n. 132, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale»

di Beatrice Fragasso

1. Segnaliamo ai lettori che il 25 settembre 2025 è stata pubblicata sulla Gazzetta Ufficiale la legge 23 settembre 2025, n. 132, contenente *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*. La legge si propone di introdurre un quadro normativo organico in materia di «ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e di modelli di intelligenza artificiale» (art. 1, c. 1), in grado di “accompagnare” – questa l’espressione utilizzata nella Relazione al d.d.l. presentato dal Governo¹ – il Regolamento 2024/1689 sull’intelligenza artificiale (c.d. AI Act)², che, come noto, rappresenta la principale fonte euro-unitaria in materia.

Per quanto in questa sede maggiormente interessa, la legge introduce diverse norme di interesse penalistico, di cui il presente contributo intende fornire un’analisi a prima lettura:

- una nuova fattispecie di *illecita diffusione di contenuti generati o manipolati artificialmente*;
- una nuova figura di reato in materia di violazione del diritto d’autore;
- una circostanza aggravante comune;
- diverse circostanze aggravanti speciali;

¹ Relazione illustrativa al d.d.l. n. S. 1146 del 2024, p. 1.

² Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull’intelligenza artificiale (c.d. AI Act). Come noto, l’AI Act detta i requisiti di sicurezza che ciascun sistema di i.a. deve soddisfare per poter essere introdotto sul mercato. In particolare, l’AI Act divide i dispositivi di intelligenza artificiale in tre categorie – a seconda del rischio che questi pongono per la sicurezza degli utenti ed il rispetto dei diritti fondamentali dei cittadini –, individuando per ciascuna categoria un regime giuridico applicabile: i sistemi di i.a. che presentano rischi considerati “inaccettabili” non potranno essere introdotti nel mercato europeo (art. 5); i sistemi ad alto rischio (artt. 6 e 7) potranno essere commercializzati, purché rispettino una serie di requisiti (artt. 8-15); per i sistemi a rischio limitato (art. 50), infine, basterà il rispetto di alcuni obblighi di trasparenza. Disposizioni specifiche sono inoltre previste per i *modelli di i.a. per finalità generali* (art. 51 ss.), ossia per quei modelli che sono «in grado di svolgere con competenza un’ampia gamma di compiti distinti» (art. 3, n. 63). Sulla struttura del Regolamento v., per tutti, i contributi contenuti in O. POLLICINO e AL. (a cura di), *La disciplina dell’intelligenza artificiale*, Giuffrè, 2025; per i profili penalistici v. M. COLACURCI, *Quale diritto penale dell’IA? Alcune riflessioni a partire dalla proposta di regolamento dell’Unione Europea*, in *Jus*, 3, 2023, p. 353 ss., e, volendo, B. FRAGASSO, [Intelligenza artificiale e responsabilità penale. Principi e categorie alla luce di una tecnologia “imprevedibile”](#), Giappichelli, 2025, p. 149 ss.

- una delega al Governo, finalizzata anch'essa, tra le altre cose, all'introduzione di nuovi reati e circostanze aggravanti³.

2. Prima di passare in rassegna le novità penalistiche, può essere utile soffermarsi brevemente sulle direttrici di fondo e sulla struttura dell'intervento normativo.

Innanzitutto, va fin da subito sottolineato che la legge in commento deve essere necessariamente letta alla luce del già menzionato Regolamento europeo sull'intelligenza artificiale. La legge 132/2025 si pone infatti in linea di continuità con il *risk-based approach* adottato dall'AI Act, prefiggendosi l'obiettivo, da un lato, di promuovere «un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale», e, dall'altro lato, di garantire «la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale» (art. 1, c. 1)⁴. Il fondamento politico-valoriale su cui poggia il Regolamento europeo – e, sulla sua scia, la legge 132/2025 – consiste infatti nell'idea che l'intelligenza artificiale possa essere all'origine di *enormi benefici sul piano dello sviluppo economico-sociale*, e che, al contempo, essa possa tuttavia essere fonte di *rischi per la tutela dei diritti fondamentali* (e se vogliamo, dal punto di vista penalistico, dei *beni giuridici*). In questo contesto, la normativa europea – di cui la legge italiana aspira ad essere complemento normativo – mira a realizzare un *bilanciamento* tra le opportunità e i rischi dello sviluppo dei sistemi di i.a.

Anche i principi generali espressi dall'art. 3 della legge hanno chiare radici nel dibattito europeo sviluppatosi intorno all'intelligenza artificiale, ripercorrendo i principi etici che costituiscono il cuore dell'AI Act. Si va dalla tutela dei diritti fondamentali (comma 1), alla necessità che nei processi di sviluppo dell'intelligenza artificiale siano garantite «la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità» (comma 2), fino all'adesione ai principi della *human-centered AI*, in base ai quali i sistemi di i.a. «devono essere sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della trasparenza, della spiegabilità», assicurando «la sorveglianza e l'intervento umano» (comma 3) e senza

³ Sul testo del d.d.l. presentato dal Governo (n. S. 1146 del 2024) v. già, limitandoci ai commenti riguardanti i profili penalistici e processual-penalistici della disciplina, B. ROMANO, *Il DDL in materia di IA: l'utilizzo nell'attività giudiziaria e in ambito sanitario*, in *Riv. it. med. leg.*, 1-2, 2024, p. 209 ss.; S. DE FLAMMINEIS, [Fattispecie penali nel contesto dell'intelligenza artificiale. Lo spunto del d.d.l. 1146/2024](#), in questa *Rivista*, 9, 2024, p. 5 ss.; G. BARONE, *La regolamentazione dell'Intelligenza Artificiale: è "corsa agli armamenti"*, in *Dir. proc. pen.*, 8, 2024, p. 991 ss.; C. PARODI, *Sistema penale e ddl sull'intelligenza artificiale: prospettive e criticità*, in *IUS penale*, p. 14 ss.; F. CONSULICH, [Il diritto penale al tempo dell'intelligenza artificiale prospettive punitive nazionali dopo l'AI Act](#), in *Dir. dif.*, 3-4, 2023, p. 721 ss., spec. p. 739 ss.; O. LOMBARDI, [Responsabilità penale dell'uomo per il danno cagionato attraverso condotte dolose e colpose nell'impiego dei sistemi di intelligenza artificiale](#), in questa *Rivista*, 12, 2024, p. 63 ss.; L. SCOLLO, *L'intelligenza artificiale entra nel Codice penale*, in *Dir. pen. proc.*, 6, 2025, p. 693 ss.

⁴ V. anche Relazione illustrativa al d.d.l. n. S. 1146 del 2024, p. 3: «Il presente disegno di legge ha l'obiettivo di operare un bilanciamento tra opportunità e rischi, prevedendo norme di principio e disposizioni di settore che, da un lato, promuovano l'utilizzo delle nuove tecnologie per il miglioramento delle condizioni di vita dei cittadini e della coesione sociale e, dall'altro, forniscano soluzioni per la gestione del rischio fondate su una visione antropocentrica».

pregiudizio per «lo svolgimento con metodo democratico della vita istituzionale e politica» (comma 4).

2.1. Sul piano della *struttura*, la legge si articola come segue:

- il Capo I (artt. 1-6) detta i principi generali che presiedono allo sviluppo e all'utilizzo dei sistemi di i.a., nonché le definizioni rilevanti ai fini dell'applicazione della legge;
- il Capo II (artt. 7-18) prevede una serie di disposizioni volte a regolare l'utilizzo dell'i.a. in diversi settori (sanità⁵, lavoro⁶, professioni intellettuali⁷, pubblica amministrazione⁸, attività giudiziaria⁹, cybersicurezza nazionale¹⁰);
- il Capo III (artt. 19-24) detta alcune norme in materia di strategia nazionale e *governance*, nonché una delega al Governo, da esercitare entro dodici mesi, avente ad oggetto, da un lato, l'adeguamento della normativa nazionale all'AI Act (art. 24, c. 1), e, dall'altro lato, la disciplina «dei casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale» (art. 24, c. 3);
- il Capo IV, contenente il solo art. 25, prevede alcune «disposizioni a tutela degli utenti e in materia di diritto d'autore»;
- il Capo V, costituito dal solo art. 26, è dedicato alle disposizioni penali;
- il Capo VI, infine, consta di due articoli: l'art. 27, che detta una clausola di invarianza finanziaria (un paradosso, se si pensa agli ingenti finanziamenti che alcuni degli interventi previsti richiederebbero), e l'art. 28, che prevede alcune disposizioni di coordinamento in relazione alla legge 28 giugno 2024, n. 90 (Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici) e prevede che l'Agenzia per la cybersicurezza nazionale – l'autorità alla quale la legge 132/2025 attribuisce le funzioni di vigilanza¹¹ – possa concludere accordi di collaborazione con soggetti privati.

3. Intelligenza artificiale e responsabilità penale: una premessa. Ora, concentrandoci sul versante penalistico, ci preme preliminarmente spendere qualche parola sull'impatto che l'intelligenza artificiale potrebbe avere sull'imputazione penale, così da poter poi valutare con maggiore ponderazione le novità penalistiche contenute nella legge¹².

⁵ Artt. 7-10, legge 23 settembre 2025, n. 132, cit.

⁶ Artt. 11-12, legge 23 settembre 2025, n. 132, cit.

⁷ Art. 13, legge 23 settembre 2025, n. 132, cit.

⁸ Art. 14, legge 23 settembre 2025, n. 132, cit.

⁹ Artt. 15-17, legge 23 settembre 2025, n. 132, cit.

¹⁰ Art. 18, legge 23 settembre 2025, n. 132, cit.

¹¹ Cfr. art. 20, lett. b), legge 132 del 2025.

¹² La letteratura sull'impatto dell'i.a. in materia penale è ormai di ampiezza considerevole. Limitandoci alle monografie pubblicate in Italia v., per quanto riguarda il settore delle auto a guida autonoma, M. LANZI, *Self-driving cars e responsabilità penale. La gestione del "rischio stradale" nell'era dell'intelligenza artificiale*, Giappichelli, 2023; R. COMPOSTELLA, *Auto a guida autonoma e diritto penale. Profili di responsabilità individuale e collettiva*, Editoriale Scientifica, 2024; nel settore dell'*healthcare*, L.A. TERRIZZI, *Medical devices e diritto penale*.

In estrema sintesi, a noi pare che lo sviluppo e l'utilizzo dei sistemi di i.a. possa sollevare due questioni di rilievo per il penalista sostanziale:

(i) per un verso, la crescente capacità di adattamento dei sistemi di i.a. più sofisticati, basati sul *machine learning*, si traduce in una certa dose di *imprevedibilità* nel "comportamento" dei dispositivi, con la conseguenza che potrebbe registrarsi una più o meno accentuata *perdita di controllo* sull'attività algoritmica: e ciò vale sia per le persone che programmano, sviluppano e mettono in commercio il prodotto intelligente, sia per coloro che lo utilizzano, o che comunque sono chiamate a supervisionarlo¹³. Una simile perdita di controllo, dal punto di vista penalistico, rischia di tradursi in una messa in crisi dei criteri ascrittivi del fatto illecito, che sono tradizionalmente fondati sul mancato dominio, da parte dell'agente, di *fatti offensivi effettivamente dominabili*. Il primo problema che si trova a dover affrontare il penalista, dunque, è quello di verificare se e in che modo l'imprevedibilità dell'intelligenza artificiale possa incidere sulla possibilità di configurare una responsabilità penale in capo alle persone che sviluppano o utilizzano l'i.a.;

(ii) per altro verso, gli *output* dell'intelligenza artificiale possono essere utilizzati per creare contenuti illeciti, o comunque contenuti che possono essere utilizzati per commettere un reato – senza, tuttavia, che l'attività algoritmica incida sulla conformazione della responsabilità penale. Si pensi al soggetto che si serva di un *chatbot* per generare un *malware* o per scrivere una mail decettiva da utilizzare nell'ambito di una campagna di *phishing*. In questi casi, l'effetto dirompente dell'intelligenza artificiale si apprezza comunque, ma in termini *quantitativi*, invece che *qualitativi*, nella misura in cui determina un incremento esponenziale delle capacità criminali degli agenti, offrendo loro sofisticatissimi strumenti tecnologici a basso costo.

Ebbene, anticipando alcune considerazioni che svilupperemo meglio più avanti, osserviamo fin da subito che la legge 132/2025 parrebbe incidere soprattutto sulla questione *sub (ii)*, introducendo figure di reato e aggravanti volte a contrastare nuove forme di aggressione a beni giuridicirealizzate *con lo strumento dell'intelligenza artificiale*. Viceversa, con riferimento al problema *sub (i)* – che è poi la questione destinata ad avere maggiori ripercussioni sul piano dell'imputazione penale –, la legge si limita a rinviare a future scelte dell'Esecutivo, attraverso la predisposizione di una delega volta ad introdurre, da un lato, delle *fattispecie di pericolo*, e, dall'altro lato, alcune *forme di limitazione della responsabilità penale* non meglio specificate.

Profili di responsabilità del produttore e dell'utilizzatore, Giuffrè, 2023; N. AMORE, *L'effetto della robotica e dell'IA nell'imputazione giuridica degli eventi infausti*, in E. ROSSERO-N. AMORE, *Robotica e intelligenza artificiale nell'attività medica. Organizzazione, autonomia, responsabilità*, il Mulino, 2023, p. 101 ss.; nella gestione d'impresa, A. MANGIONE, *Intelligenza artificiale, attività d'impresa e diritto penale. La «funzione di garanzia» nell'organizzazione e dell'organizzazione per la «sorveglianza dell'AI»*, Giappichelli, 2024; per un approccio trasversale ai vari settori di applicazione dell'i.a. v. A. GIANNINI, *Criminal behavior and Accountability of Artificial Intelligence Systems*, Eleven, 2023; L. D'AMICO, *La misura della (im)prevedibilità. Modelli d'imputazione della responsabilità al tempo dell'intelligenza artificiale*, ESI, 2025; volendo, v. anche B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit.

¹³ Sul c.d. "problema del controllo" v. più ampiamente B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit., p. 43 ss.

4. La definizione di “sistema di intelligenza artificiale”. Delineate, seppur cursoriamente, le implicazioni che l’intelligenza artificiale potrebbe avere sulla responsabilità penale, passiamo ora all’esame delle disposizioni contenute nella nuova legge 132/2025.

Una prima norma di interesse, sul piano (anche) penalistico, è quella che circoscrive la nozione di “sistema di i.a.” rilevante ai fini dell’applicazione della legge. Tutte le figure di reato e le circostanze aggravanti introdotte dal provvedimento hanno infatti in comune il riferimento al “sistema di i.a.” quale elemento normativo; e lo stesso vale per le disposizioni che saranno introdotte in attuazione della delega al Governo «per adeguare e specificare la disciplina dei casi di realizzazione e di impiego illecit[o] di sistemi di intelligenza artificiale» (art. 24, c. 3). Una riflessione sulla definizione di “sistema di i.a.” adottata dalla legge è dunque d’obbligo, e preliminare rispetto alla disamina delle singole disposizioni penalistiche.

La legge 132/2025, in particolare, rinvia all’art. 3, par. 1, n. 1, AI Act, che definisce un “sistema di i.a.” come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall’*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

Non è questa la sede per ripercorrere i dibattiti che hanno accompagnato l’adozione, a livello europeo, di una simile definizione: basterà dire che la delimitazione del campo di applicazione dell’AI Act è stata una delle questioni più discusse nell’ambito delle negoziazioni tra Commissione, Parlamento e Consiglio dell’Unione europea¹⁴, e che anche l’attuale norma definitoria continua a generare alcune perplessità in ordine alla sua reale capacità di circoscrivere con chiarezza l’ambito di applicazione del regolamento. In particolare, come non ha mancato di mettere in luce la dottrina, in questa definizione rientreranno probabilmente anche sistemi che normalmente, oggi, non sono considerati come “intelligenti”, e che magari sono già in circolazione da tempo¹⁵.

4.1. L’adozione di una nozione così ampia di intelligenza artificiale anche in materia penalistica comporta evidentemente che le nuove aggravanti e fattispecie incriminatrici siano destinate ad applicarsi anche in relazione a dispositivi tecnologici la cui produzione e il cui utilizzo non siano caratterizzati da una pericolosità maggiore (o comunque qualitativamente diversa) rispetto alla produzione e all’utilizzo di tecnologie tradizionali. Il rischio, dunque, è che le nuove norme – pensate per rispondere a quell’*imprevedibilità* che connota l’intelligenza artificiale, e che ha evidentemente effetti

¹⁴ Sulle modifiche subite dalla norma definitoria nel corso del processo di approvazione del regolamento, v. diffusamente C. TRINCADO CASTAN, *The legal concept of artificial intelligence: the debate surrounding the definition of AI System in the AI Act*, in *BioLaw Journal – Riv. BioDiritto*, 1, 2024, p. 305 ss.

¹⁵ In questo senso v., per tutti, J. MÖKANDER E AL., *Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Pro- posed European AI Regulation*, in *Minds and Machines*, 32, 2022, p. 245.

dirompenti per l'imputazione penale – finiscano per applicarsi anche in relazione a sistemi tecnologici che potrebbero non necessitare di un intervento legislativo *ad hoc*.

Nonostante ciò, la scelta del legislatore di rinviare alla definizione europea ci sembra, nel complesso, condivisibile.

Sono noti gli sforzi di scienziati, studiosi e *rule makers* per individuare una nozione di i.a. che sia al tempo stesso omnicomprensiva e sufficientemente delimitativa del fenomeno – sforzi che hanno avuto come risultato l'affastellarsi, talvolta nell'ambito del medesimo settore disciplinare, di una pletera di diverse proposte definitorie, spesso vaghe e sfuggenti¹⁶. Benché effettivamente la definizione fornita dall'AI Act paia lontana dai crismi della determinatezza, il beneficio del rinvio sta nel fatto che tale norma definitoria è destinata, nel corso dei prossimi anni, ad una massiccia applicazione e – si auspica – ad un'accurata opera di interpretazione da parte degli organismi della *governance* europea. I consociati – e i giudici – dovrebbero dunque poter contare, sul lungo periodo, su criteri stabili per valutare se il dispositivo possa essere qualificato o meno come sistema di i.a.

Nell'immediato, invece, la questione è più complicata. Se è vero che potranno essere classificati agevolmente come sistemi di i.a. tutti quei dispositivi che siano stati immessi sul mercato attraverso le procedure previste dall'AI Act, la qualificazione potrà essere più ostica nel caso di dispositivi acquisiti su circuiti illeciti – circostanza che, d'altra parte, non può di certo considerarsi peregrina, specialmente in relazione a forme di criminalità dolosa. Possiamo prevedere, in questo contesto, che la riconduzione dei *device* utilizzati dagli imputati alla nozione di "intelligenza artificiale" costituirà uno dei principali snodi interpretativi sui quali si confronteranno le parti del processo.

5. Illecita diffusione di contenuti generati o manipolati artificialmente (art. 612-quater c.p.). La prima tra le fattispecie di reato introdotte dalla legge 132/2025 è quella di *Illecita diffusione di contenuti generati o manipolati artificialmente* (art. 612-quater c.p.), che punisce con la reclusione da uno a cinque anni «[c]hiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità». Il delitto è punibile a querela della persona offesa, salvo che il fatto sia connesso con un altro delitto per il quale si deve procedere d'ufficio oppure sia «commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate».

5.1. L'obiettivo principale della fattispecie parrebbe quello di reprimere la diffusione non consensuale di *deepfakes* – ove per *deepfake* si intende, secondo la definizione fornita dall'AI Act, «un'immagine o un contenuto audio o video generato o

¹⁶ Sulla complessità della questione definitoria, nell'ambito degli stessi settori afferenti alla *computer science*, sia consentito il rinvio a B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit., p. 17 ss.

manipolato dall'IA che assomiglia a persone, oggetti, luoghi o altre entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona»¹⁷.

Stante l'indeterminatezza nella descrizione dell'evento, si deve ritenere che il danno ingiusto non debba necessariamente avere un contenuto patrimoniale¹⁸. A sostegno di tale interpretazione vi è la collocazione topografica all'interno del codice – tra i delitti contro la libertà morale –, nonché la stessa relazione illustrativa al testo del d.d.l. presentato dal Governo, che sottolinea come la fattispecie miri ad offrire «una tutela rafforzata della persona, incentrando l'offensività della condotta sul pregiudizio all'autodeterminazione ed al pieno svolgimento della personalità»¹⁹.

Scopo di tutela della fattispecie sembrerebbe essere costituito, innanzitutto, dalle condotte di diffusione non consensuale di *deepfakes porn*, ovvero sia di immagini manipolate in cui fotografie o video raffiguranti dei visi riconoscibili vengono “innestati” su immagini di corpi di altri soggetti, nudi o impegnati in atti di natura esplicitamente sessuale²⁰.

Nel nostro ordinamento, effettivamente, sembrerebbero mancare, *de iure condito*, delle disposizioni specificamente applicabili a tali condotte. Nella nozione di «immagini o video a contenuto sessualmente esplicito» contenuta nel reato di *Diffusione illecita di immagini o video sessualmente espliciti* (art. 612-ter c.p.) non sembrerebbero infatti inclusi i *deepfakes*²¹. A tale conclusione si giunge ove si consideri che il legislatore italiano, quando ha voluto, ha dato esplicito e autonomo rilievo alle immagini manipolate: si pensi, in particolare, all'art. 600-*quater*.1 c.p., che stabilisce che i reati di pornografia minorile (artt. 600-*ter* e 600-*quater* c.p.) si applicano – con pena diminuita – anche quando il materiale pornografico «rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse» (c. 1), ove per “immagini virtuali” si intendono le «immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali» (c. 2).

¹⁷ V. art. 3, par. 1, n. 60, AI Act, cit.

¹⁸ In questo senso, F. CONSULICH, [Il diritto penale al tempo dell'intelligenza artificiale prospettive punitive nazionali dopo l'AI Act](#), cit., p. 740; S. DE FLAMMINEIS, [Fattispecie penali nel contesto dell'intelligenza artificiale](#), cit., p. 9.

¹⁹ Relazione illustrativa al d.d.l. n. S. 1146 del 2024, cit., p. 16.

²⁰ Sul fenomeno e sulle prospettive di regolazione dei *deepfakes porn v.*, per tutti, C. SALVI, *Emerging trends in criminalising deepfake pornography: challenges and perspectives*, in G. VERMEULEN – N. PERSÖAK – S. DE COENSEL (eds.), *Researching the boundaries of Sexual integrity, gender violence and image-based abuse*, in *Revue Internationale de Droit Pénal*, 95, 2, 2024, p. 5 ss.; G.M. CALETTI, *Habeas corpus digitale. Lo statuto penale dell'immagine corporea tra privacy e riservatezza*, Giappichelli, 2024, p. 157 ss.; M. PICCARDI, *L'impatto del deepfake sul diritto penale*, in A. CADOPPI – S. CANESTRARI – A. MANNA – M. PAPA (a cura di), *Cybercrime*, II ed., Utet, 2023, p. 1462 ss.; C. PAONESSA, [La diffusione di contenuti illeciti online. Obblighi di incriminazione e contrasto del “deepfake” nella Direttiva \(UE\) 2024/1385](#), in *disCrimen*, 10 giugno 2025, in corso di pubblicazione in *Criminalia*. Cfr. anche il report di Europol, [Facing reality? Law enforcement and the challenge of deepfake. An Observatory Report from the Europol Innovation Lab](#), 2022, aggiornato il 13 marzo 2024.

²¹ A. GULLO-R. FLOR, *Italian report on criminalisation of AI-related offences*, in F. MIRÓ-LLINARES – C. DUVAC – T. TOADER – M. SANTISTEBAN GALARZA (eds.), *Criminalisation of AI-related offences. International Colloquium, Bucharest, Romania, 14-16 June 2023*, in *Revue Internationale de Droit Pénal*, 95, 1, 2024, p. 193.

Prima che venisse approvata la legge 132/2025, dunque, una tutela penalistica specifica contro la diffusione di *deepfakes porn* sussisteva soltanto nel caso in cui la persona offesa fosse un minore.

L'introduzione di una fattispecie in grado di sanzionare la diffusione non consensuale di immagini manipolate sessualmente esplicite è certamente da salutare con favore, dal momento che tale condotta – oltre che costituire un'offesa alla reputazione – costituisce altresì un'aggressione all'intimità, alla riservatezza e all'autodeterminazione nel campo della sfera sessuale individuale, non meno di quanto lo siano le condotte punite ai sensi dell'art. 612-ter c.p.²². La sanzione penale per la diffusione di *deepfakes porn*, tuttavia, avrebbe forse potuto passare, in maniera più lineare, per la formulazione di una fattispecie *di condotta* specificamente ritagliata su tale ipotesi.

Si tenga presente, a tal proposito, che l'introduzione di uno specifico reato *di condotta*, volto a punire la diffusione di immagini manipolate sessualmente esplicite, è prevista anche dalla Direttiva europea 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica²³, che richiede agli Stati membri che venga incriminata la seguente condotta intenzionale: «produrre, manipolare o alterare e successivamente rendere accessibile al pubblico, tramite TIC²⁴, immagini, video o analogo materiale in modo da far credere che una persona partecipi ad atti sessualmente espliciti, senza il consenso della persona interessata, qualora tali condotte possano arrecare un danno grave a tale persona»²⁵.

La previsione dell'evento di danno, quale elemento del reato, parrebbe dunque costituire un requisito ultroneo rispetto a quanto stabilito dalla direttiva.

5.2. Se la legge 132/2025 ha optato per una formulazione non specificamente tarata sul fenomeno della diffusione non consensuale di *deepfakes porn* è probabilmente perché il raggio d'azione della nuova fattispecie ambisce ad essere più ampio.

Ci riferiamo, in particolare, alla possibile applicazione del reato in esame in relazione all'utilizzo di *deepfakes* a scopo di propaganda politica o di disinformazione. Le declinazioni di tale utilizzo sono le più varie: ci limitiamo qui a menzionare, a mero titolo di esempio, il video manipolato che raffigura il Primo ministro ucraino Volodymyr

²² Il dibattito su quale sia il bene giuridico offeso dalla diffusione di *deepfakes porn* è in realtà molto sfaccettato; v., a tal proposito, C. SALVI, *Emerging trends in criminalising deepfake pornography: challenges and perspectives*, cit., p. 9.

²³ Direttiva (UE) 2024/1385 del Parlamento europeo e del Consiglio del 14 maggio 2024 sulla lotta alla violenza contro le donne e alla violenza domestica; in argomento v. S. BRASCHI, *La nuova direttiva sulla lotta alla violenza contro le donne e alla violenza domestica e le sue ricadute nell'ordinamento nazionale*, in *Dir. pen. proc.*, 10, 2024, p. 1367 ss.; A. MASSARO, [La Direttiva UE 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica: il possibile impatto sull'ordinamento italiano](#), in questa *Rivista*, 3, 2025, p. 107 ss.

²⁴ Tecnologie dell'informazione e della comunicazione.

²⁵ Art. 5, par. 1, lett. b), direttiva (UE) 2024/1385 sulla lotta alla violenza contro le donne e alla violenza domestica, cit. Sull'inclusione, in tale fattispecie, della generazione e della diffusione non consensuale di *deepfakes porn* v. il considerando 19: «Nel concetto di produzione, manipolazione o alterazione dovrebbe rientrare anche la fabbricazione di video fasulli ma realistici («deepfake») con persone, oggetti, luoghi o altre entità o eventi molto simili a quelli realmente esistenti, che ritraggono una persona mentre compie atti sessuali, risultando falsamente autentici o veritieri agli occhi altrui».

Zelensky che invita i cittadini a deporre le armi e ad arrendersi di fronte all'invasione russa, o al video che riproduce artificialmente il Presidente russo Vladimir Putin che ordina il ritiro delle truppe dal suolo ucraino²⁶.

Un indice nel senso di ritenere che queste siano le intenzioni del legislatore può essere tratto dal secondo comma dell'art. 612-*quater* c.p., che stabilisce che si procede d'ufficio, tra le altre ipotesi, quando il delitto è commesso nei confronti «di una pubblica autorità a causa delle funzioni esercitate»²⁷.

L'evento-danno rilevante ai fini della configurazione del reato potrebbe essere, in questi casi, il danno alla reputazione. Va tuttavia osservato che, come già rilevato in dottrina, l'utilizzo di *deepfakes* per fini di propaganda politica s'inserisce in un più ampio fenomeno di manipolazione digitale del consenso, realizzata con o senza l'intelligenza artificiale, e che è capace di incidere sul corretto funzionamento delle istituzioni democratiche²⁸. Con riferimento a queste ipotesi, insomma, un reato di danno rischia di essere, come è stato osservato, "inadeguato per difetto"²⁹.

Il riferimento, nell'art. 612-*quater* c.p., alla causazione di un generico danno ci pare in ogni caso eccessivamente indeterminato: una più precisa identificazione dei beni giuridici offesi avrebbe reso il reato maggiormente aderente ai principi di legalità e offensività³⁰.

6. Modifiche alla legge 22 aprile 1941, n. 633, in materia di diritto d'autore. Anche tra le modifiche apportate alla legge 22 aprile 1941, n. 633, sul diritto d'autore, vi sono alcuni interventi di interesse penalistico.

6.1. Segnaliamo, innanzitutto, che la legge sull'i.a. precisa il campo di applicazione della legge 633/1941, specificando che la protezione garantita da quest'ultimo provvedimento si intende riferita alle sole opere di ingegno «umane», anche laddove «create con l'ausilio di strumenti di intelligenza artificiale, purché

²⁶ Sull'utilizzo di *deepfakes* nel contesto specifico della disinformazione e della propaganda politica v. C. SALVI, *The Challenges of Deepfake Technology in the Context of Political Disinformation*, in M. BERGSTRÖM – V. MITSILEGAS (eds.), *EU Law in the Digital Age*, Hart, 2025, p. 185 ss.; T. GUERINI, *Fake news e diritto penale*, Giappichelli, 2020, p. 45 ss.; ID., *Disinformation, Fake News and Deep Fakes*, in F. MIRÓ-LLINARES – C. DUVAC – T. TOADER – M. SANTISTEBAN GALARZA (eds.), *Criminalisation of AI-related offences*, cit., p. 114 ss.

²⁷ Cfr. in questo senso O. LOMBARDI, [Responsabilità penale dell'uomo per il danno cagionato attraverso condotte dolose e colpose nell'impiego dei sistemi di intelligenza artificiale](#), cit., p. 64.

²⁸ In argomento v., per tutti, T. GUERINI, *Fake news e diritto penale*, cit., *passim*, e P. GUERCIA, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. CADOPPI – S. CANESTRARI – A. MANNA – M. PAPA (a cura di), *Cybercrime*, cit., p. 1290 ss., ai quali si rinvia per un esame delle proposte di legge presentate in Italia e all'estero per contrastare il fenomeno della disinformazione.

²⁹ Così F. CONSULICH, [Il diritto penale al tempo dell'intelligenza artificiale prospettive punitive nazionali dopo l'AI Act](#), cit., p. 740.

³⁰ Cfr., in questo senso, G. FIORINELLI, *La violenza mediata dalla tecnologia. Dogmatica, profili politico-criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Giappichelli, 2024, pp. 304-305, che parla di «omnicomprensivo (quanto pericoloso) veicolo di una repressione penale illimitata e paracivilistica dei "danni" cagionati mediante l'intelligenza artificiale generativa, risultando quindi maldestra reazione simbolica a un fenomeno di crescente allarme sociale».

costituenti risultato del lavoro intellettuale dell'autore»³¹. Ne risulta precisato, di conseguenza, anche il campo di applicazione dei reati contenuti nella medesima legge, che puniscono la diffusione e la riproduzione senza diritto di opere d'ingegno (v., in particolare, gli artt. 171 ss.). Va detto, tra l'altro, che difficilmente può parlarsi di una vera e propria modifica di un elemento normativo delle fattispecie, atteso che nella nozione di "opere di ingegno" ci pare che già potesse ritenersi implicito il requisito della derivazione "umana" della creazione.

6.2. Sempre in materia di diritto d'autore, la legge 132/2025 introduce poi una nuova fattispecie all'art. 171, c. 1, lett. a-ter, l. 22 aprile 1941, n. 633, che punisce chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma, «riproduce o estrae testo o dati da opere o altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-ter e 70-quater, anche attraverso sistemi di intelligenza artificiale». La figura di reato si va ad aggiungere alle fattispecie già previste dall'art. 171 l. 633/1941 in materia di violazione del diritto d'autore; come queste ultime, la nuova fattispecie è punita con la pena della multa da 51 a 2.065 euro, e si applica salvo quanto previsto dagli artt. 171-bis e 171-ter (che puniscono, rispettivamente, la duplicazione di "programmi per elaboratore" e la diffusione abusiva, per uso non personale, di opere letterarie, scientifiche, cinematografiche, etc.).

La nuova figura di reato mira a contrastare il fenomeno del c.d. *data scraping*, ovvero di quella pratica di estrazione massiva, indiscriminata e non autorizzata di contenuti pubblicati *online*, finalizzata ad addestrare i modelli di i.a. Si badi, a tal proposito, che la nuova fattispecie – coerentemente con il bene giuridico che si propone di tutelare – punisce esclusivamente l'estrazione e la riproduzione di *dati protetti da diritto d'autore*: tale condotta, come noto, è stata oggetto di ampi dibattiti, negli ultimi anni, soprattutto in relazione alle attività della società OpenAI, accusata di aver addestrato uno dei più noti sistemi di i.a. generativa, ChatGPT, grazie all'utilizzo non autorizzato di articoli e libri scientifici³² e di contributi pubblicati sui siti dei quotidiani³³.

Non rientrano, invece, nel campo di applicazione della fattispecie le condotte di estrazione e riproduzione, senza base giuridica, di *dati personali* presenti *online* – condotte che, già da qualche anno, sono comunque oggetto di attenzione da parte del

³¹ V. art. 1, c. 1, legge 22 aprile 1941, n. 633, così come modificato dall'art. 25, c. 1, lett. a): «Sono protette ai sensi di questa legge le opere dell'ingegno *umano* di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione, *anche laddove create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del lavoro intellettuale dell'autore*» (le modifiche sono indicate in corsivo).

³² Si consideri, a tal proposito, che secondo diverse fonti i libri e gli articoli erano stati scaricati dalle c.d. *shadow libraries*, ovvero archivi digitali nei quali vengono messi a disposizione gratuitamente, e in violazione del diritto d'autore, testi protetti da *copyright*; in argomento v. E. CREAMER, [Authors file a lawsuit against OpenAI for unlawfully 'ingesting' their books](#), in *The Guardian*, 5 luglio 2023.

³³ Probabilmente la vicenda più nota è quella che ha visto coinvolto il New York Times, che nel dicembre 2023 ha presentato ricorso contro OpenAI per alcune presunte violazioni in materia di *copyright*; in argomento v. M.M. GRYNBAUM – R. MAC, [The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work](#), in *The New York Times*, 27 dicembre 2023.

Garante per la protezione dei dati personali, che in almeno due casi ne ha dichiarato l'illiceità, per violazione di diverse disposizioni del Regolamento (UE) 2016/679 (GDPR)³⁴.

7. Le nuove circostanze aggravanti. Tra gli interventi previsti dalla legge 132/2025 vi è poi l'introduzione di un'aggravante comune e di alcune aggravanti speciali.

7.1. L'aggravante comune si va ad aggiungere, al n. 11-*decies*, al lungo elenco di circostanze previste all'art. 61, c. 1, c.p. In particolare, l'aggravante si applica ai casi in cui il fatto sia stato commesso «mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato».

Si noti, per inciso, che, nelle more dell'approvazione definitiva della legge sull'i.a., un nuovo n. 11-*decies* era già stato aggiunto all'art. 61 c.p. dall'art. 11, c. 1, d.l. 11 aprile 2025, n. 48 (c.d. decreto sicurezza), conv. in l. 9 giugno 2025, n. 80, per i reti commessi all'interno o nelle adiacenze delle stazioni ferroviarie e dei treni³⁵. Oggi, di conseguenza, l'art. 61 c.p. *contiene due n 11-decies*: una svista che richiederebbe un pronto intervento di rinumerazione da parte del legislatore, al fine di evitare incertezze nella contestazione e nell'applicazione delle aggravanti³⁶.

7.2. L'art. 26 della legge prevede poi l'introduzione di alcune circostanze aggravanti speciali per l'aver commesso il fatto mediante l'impiego di sistemi di i.a. Le fattispecie aggravate, in particolare, sono le seguenti: attentati contro i diritti politici del cittadino (art. 294 c.p.), aggioaggio (art. 2637 c.c.), manipolazione del mercato (art. 185, d.lgs. 24 febbraio 1998, n. 58)³⁷.

³⁴ Garante per la protezione dei dati personali, [Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 \[9751362\]](#), Registro dei provvedimenti n. 50 del 10 febbraio 2022; Id., [Provvedimento del 17 maggio 2023 \[9903067\]](#), Registro dei provvedimenti n. 201 del 17 maggio 2023.

³⁵ Questo il testo dell'aggravante introdotta dal c.d. decreto sicurezza: «l'aver, nei delitti non colposi contro la vita e l'incolumità pubblica e individuale, contro la libertà personale e contro il patrimonio, o che comunque offendono il patrimonio commesso il fatto all'interno o nelle immediate adiacenze delle stazioni ferroviarie e delle metropolitane o all'interno dei convogli adibiti al trasporto di passeggeri».

³⁶ *Aggiornamento* – Segnaliamo che, in un momento successivo rispetto alla pubblicazione di questo articolo, l'errore materiale è stato corretto, e la nuova aggravante sull'impiego di sistemi di i.a. è stata collocata al n. 11-*undecies* dell'art. 61 c.p.; v. l'avviso di rettifica contenuto nella [Gazzetta Ufficiale, Serie generale n. 242 del 17 ottobre 2025](#).

³⁷ Si badi, a quest'ultimo proposito, che la legge identifica, quale pena "aggravata" per la manipolazione del mercato realizzata attraverso sistemi di i.a., la pena della reclusione dai due ai sette anni, mentre la pena base della fattispecie va *dai due ai dodici anni*. Si tratta, evidentemente, di una svista del legislatore, che tuttavia è in grado di creare un cortocircuito di non poco momento nella disciplina degli abusi di mercato. Sul tema rinviamo alle considerazioni più approfondite F. MUCCIARELLI, [Intelligenza artificiale e condotte manipolative su strumenti finanziari: una nuova aggravante con effetto attenuante](#), in questa Rivista.

7.3. Notiamo, innanzitutto, nei rapporti tra circostanze speciali e circostanza comune, che con riferimento a quest'ultima non sarà sufficiente il mero utilizzo di un sistema di i.a. per commettere il reato, ma sarà necessaria la dimostrazione di un *quid pluris* di offensività derivante dall'uso del dispositivo intelligente: o in forza della peculiare insidiosità del mezzo, o perché tale mezzo – anche se non insidioso – ha «comunque ostacolato la pubblica o la privata difesa», oppure, ancora, perché l'utilizzo del sistema di i.a. ha aggravato le conseguenze del reato. Di converso, ai fini dell'applicabilità delle aggravanti speciali, sarà sufficiente che l'agente abbia utilizzato i sistemi di i.a., considerati *ex se* come “strumenti” insidiosi per l'aggressione ai beni giuridici tutelati dalle fattispecie incriminatrici³⁸: una soluzione che non convince del tutto, dal momento che l'ampia definizione di intelligenza artificiale adottata dalla legge – sulla quale v. *supra*, par. 4. ss. – include anche tecnologie che non possono presumersi, in via assoluta, come più pericolose o insidiose rispetto alle ordinarie modalità di commissione dei reati.

D'altra parte, bisogna guardarsi da facili illusioni. La principale peculiarità dei sistemi di i.a., rispetto ai precedenti dispositivi tecnologici, è infatti – lo si è già detto – quella di sfuggire al pieno controllo dell'agente umano, con il risultato che l'intelligenza artificiale potrebbe incidere sulla stessa configurabilità della responsabilità penale in capo all'agente; prima ancora, dunque, che possa discutersi dell'applicabilità o meno delle circostanze aggravanti³⁹.

Ecco, dunque, che se in un caso di truffa attuata con l'utilizzo di *deepfakes*⁴⁰ l'intelligenza artificiale pare davvero come uno strumento nelle mani dell'utilizzatore, lo stesso potrebbe non accadere in relazione alle fattispecie di agguato o di manipolazione del mercato. L'algoritmo di *trading* potrebbe infatti esercitare, in alcune ipotesi, un vero e proprio *decision making* nell'identificazione delle strategie di acquisto e vendita di titoli, con la conseguenza che l'attività dell'i.a. potrebbe fuoriuscire dalla sfera della *rappresentazione e volizione* dell'operatore umano⁴¹.

³⁸ In questo senso v. S. DE FLAMMINEIS, [Fattispecie penali nel contesto dell'intelligenza artificiale](#), cit., p. 8.

³⁹ Cfr. F. CONSULICH, [Il diritto penale al tempo dell'intelligenza artificiale prospettive punitive nazionali dopo l'AI Act](#), cit., pp. 740-741.

⁴⁰ L'ipotesi che i *deepfake* vengano utilizzati per finalità fraudolente è tutt'altro che teorica. Emblematico, a tal proposito, è il caso della truffa realizzata da alcune persone che, simulando – tramite l'utilizzo di un *deepfake* – la voce del Ministro della Difesa Guido Crosetto, avevano contattato diversi imprenditori italiani convincendoli a versare somme di denaro, con il pretesto di dover pagare presunti riscatti per alcuni giornalisti rapiti in Medio Oriente; in argomento v. Redazione Il Post, [Le indagini sui truffatori che fingevano di essere il ministro Crosetto](#), in *Il Post*, 11 febbraio 2025.

⁴¹ Sull'impatto dell'imprevedibilità algoritmica sulla responsabilità penale dolosa – un argomento che, fino ad ora, ha ricevuto poche attenzioni in dottrina – ci siamo concentrati diffusamente in B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit., p. 543 ss., a cui rinviamo; tra gli Autori che già si sono occupati ampiamente della materia, con particolare riferimento alla manipolazione del mercato “algoritmica”, imprescindibile è il riferimento a F. CONSULICH, *Flash offenders. Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. proc. pen.*, 3, 2022, p. 1031 ss.; Id., *Il nastro di Mobius, Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa*, 71, 2, 2018, p. 195 ss.

8. Le deleghe al Governo in materia penale. Se in ambito doloso il legislatore sembra concepire il sistema di i.a. come mero *strumento* per la commissione di reati, diversa sembra la consapevolezza circa i rischi dell'i.a. per quanto riguarda l'imputazione colposa. È da questo punto di osservazione che, a nostro avviso, va letta la delega al Governo prevista dalla legge 132/2025.

In particolare, l'art. 24 prevede, al comma 3, che il Governo sia delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della legge, «uno o più decreti legislativi per adeguare e specificare la disciplina dei casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale». A tal fine, il comma 5 elenca una serie di principi e criteri direttivi, di cui ci limitiamo a menzionare quelli di interesse strettamente penalistico⁴²:

- «previsione di strumenti, anche cautelari, finalizzati a inibire la diffusione e a rimuovere contenuti generati illecitamente anche con sistemi di intelligenza artificiale, assistiti da un sistema di sanzioni effettive, proporzionate e dissuasive» (lett. a)
- «introduzione di autonome fattispecie di reato, punite a titolo di dolo o di colpa, incentrate sull'omessa adozione o sull'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato» (lett. b);
- «precisazione dei criteri di imputazione della responsabilità penale delle persone fisiche e amministrativa degli enti per gli illeciti inerenti a sistemi di intelligenza artificiale, che tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente» (lett. c);
- «modifica, a fini di coordinamento e di razionalizzazione del sistema, della normativa sostanziale e processuale vigente, in conformità ai principi e ai criteri enunciati nelle lettere a), b), c), d) ed e)» (lett. f).

8.1. Innanzitutto, non si può non rilevare come la delega, in molte delle sue parti, sia ben lontana da quegli standard di analiticità e chiarezza che soli potrebbero giustificare il ricorso, in materia penale, alla delega legislativa – e il tema è ancora più delicato se si considera che, come ormai è prassi, il provvedimento è di iniziativa governativa.

Gravemente deficitario, sul piano della determinatezza, è senz'altro il criterio indicato nella lett. a), che prevede l'introduzione di «strumenti, anche cautelari,

⁴² Al di fuori delle previsioni di interesse sotto il profilo di diritto penale sostanziale, l'art. 24, c. 5, legge 132/2025 prevede inoltre i seguenti criteri direttivi «d) nei casi di responsabilità civile, previsione di strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dal regolamento (UE) 2024/1689; e) regolazione dell'utilizzo dei sistemi di intelligenza artificiale nelle indagini preliminari, nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza».

finalizzati a inibire la diffusione e a rimuovere contenuti generati illecitamente anche con sistemi di intelligenza artificiale, assistiti da un sistema di sanzioni effettive, proporzionate e dissuasive». Anche volendo sorvolare sulla farraginosità della formulazione – che pretende che delle «sanzioni effettive, proporzionate e dissuasive» possano “assistere” un’attività avente contenuto cautelare –, non si può non rilevare come la definizione di quali siano le condotte illecite meritevoli di sanzione (e, dunque, del precepto penale) sia demandata *in toto* al Governo, con grave *vulnus* per il principio di riserva di legge in materia penale.

Non è del tutto chiaro, inoltre, se l’espressione “anche con sistemi di intelligenza artificiale” sia riferita agli *strumenti di inibizione o rimozione dei contenuti* o ai *contenuti generati illecitamente*, e, di conseguenza, se l’i.a. debba, in questa sede, essere considerata come un possibile supporto alle autorità di contrasto, oltre che come uno strumento di generazione di contenuti illeciti. L’utilizzo del termine “anche” ci induce ad escludere che la precisazione sia da associare al sintagma “contenuti generati illecitamente” – atteso che l’utilizzo dell’i.a. sembrerebbe essere elemento *necessario*, e non invece accessorio, degli illeciti di cui si richiede l’introduzione.

Se abbiamo inteso correttamente l’*intentio legis*, dunque, l’obiettivo della disposizione è quello di consentire l’impiego dell’i.a. nell’ambito dell’attività di *law enforcement*. Tale prospettiva – da leggersi congiuntamente alle disposizioni della legge 132/2025 che regolano l’utilizzo dell’i.a. in ambito giudiziario⁴³ – apre evidentemente una serie di interrogativi su come garantire che gli *output* algoritmici siano sempre sottoposti al vaglio critico della persona responsabile del procedimento, e al contempo che tali *output* possano essere messi in discussione dai soggetti interessati, conformemente al principio del giusto processo e al diritto di difesa.

8.2. Centrale, nella struttura dell’intervento normativo, è senz’altro la delega volta ad introdurre delle fattispecie, punite a titolo di dolo o di colpa, incentrate

⁴³ Cfr. art. 15, legge 23 settembre 2025, n. 132, cit. Segnaliamo, a tal proposito, che, nel corso del dibattito parlamentare, le maglie della possibile applicazione dell’intelligenza artificiale nel settore della giustizia sembrerebbero essersi allargate, comprendendo la possibilità di avvalersi di sistemi di i.a. anche a supporto della decisione giudiziaria in senso stretto (seppur con la precisazione che «è sempre riservata al magistrato ogni decisione sull’interpretazione e sull’applicazione della legge, sulla valutazione dei fatti e delle prove e sull’adozione dei provvedimenti»); così il primo comma dell’art. 15). Viene superata, in particolare, la limitazione che era prevista dall’art. 14, c. 1, del precedente testo, che stabiliva che «[i] sistemi di intelligenza artificiale sono utilizzati *esclusivamente* per l’organizzazione e la semplificazione del lavoro giudiziario, nonché per la ricerca giurisprudenziale e dottrinale» (enfasi aggiunta). Com’era stato rilevato dai primi commenti al testo del d.d.l. presentato dal Governo, una simile limitazione avrebbe effettivamente ridotto di molto gli orizzonti applicativi tracciati, nel settore della giustizia, dall’AI Act e dalla Carta etica europea sull’utilizzo dell’intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi (redatta dalla Commissione europea per l’efficienza della giustizia e approvata dal Consiglio d’Europa il 3 dicembre 2018), che prevedono la possibilità, per i magistrati, di avvalersi di sistemi di i.a. a supporto dell’attività giudiziaria, seppur nel rispetto di rigorose garanzie volte a tutelare i diritti fondamentali, l’autonomia del giudice e la trasparenza delle decisioni. In argomento, con riferimento al testo inizialmente presentato dal Governo, cfr. G. CANZIO, [Al act e processo penale: sfide e opportunità](#), in questa *Rivista*, 14 ottobre 2024, par. 6; G. BARONE, *La regolamentazione dell’Intelligenza Artificiale: è “corsa agli armamenti”*, cit., p. 1000.

«sull’omessa adozione o sull’omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l’utilizzo professionale di sistemi di intelligenza artificiale, quando da tali omissioni deriva pericolo concreto per la vita o l’incolumità pubblica o individuale o per la sicurezza dello Stato» (lett. b). È in questa disposizione, a nostro parere, che si coglie la consapevolezza che le fattispecie che puniscono eventi di danno potrebbero risultare inadeguate a sanzionare la condotta degli utilizzatori e dei produttori dei sistemi di i.a., e che, di conseguenza, potrebbe essere necessaria l’introduzione di reati che anticipino la tutela penale allo stadio della *creazione del pericolo*.

Sebbene la scelta del legislatore ci paia tendenzialmente condivisibile, nella misura in cui consente di mantenere un presidio penalistico in un settore in cui sono evidenti i rischi di deresponsabilizzazione di produttori e utilizzatori, non può sottacersi come la tecnica del pericolo concreto richiamata dalla norma renda pur sempre necessario, per il giudice, l’accertamento dell’esistenza di un *pericolo illecito*, nonché del *nesso tra violazione cautelare e pericolo*: valutazioni, quelle menzionate, che potrebbero rivelarsi tutt’altro che immediate, stante l’opacità e l’inesplicabilità che attualmente caratterizzano i risultati algoritmici⁴⁴.

8.3. Quanto ai criteri descritti dalla lett. c), obiettivo del legislatore sembrerebbe quello di delimitare la responsabilità penale, piuttosto che imporre nuove fattispecie o aggravanti: in questo senso inducono a ritenere l’utilizzo del termine “precisare” – che rimanda ad una funzione limitativa rispetto all’area del penalmente rilevante – e il riferimento al “livello effettivo di controllo”, che sembrerebbe voler dar rilievo a forme di inesigibilità nell’esercizio della sorveglianza sull’algoritmo.

La finalità della delega è senz’altro condivisibile. In un contesto di crescente *perdita di controllo* sull’attività algoritmica, la persona fisica incaricata della supervisione del sistema di i.a. rischia di diventare il capro espiatorio dell’intera regolazione dell’intelligenza artificiale. Il supervisore, infatti, pur essendo gravato da un *obbligo di sorveglianza*, potrebbe, nei fatti, risultarne *privo*, stante il tipico *deficit* di controllabilità che caratterizza i rapporti tra sistemi di i.a. ed esseri umani⁴⁵.

La via più immediata per l’attuazione della delega consiste nella limitazione della responsabilità penale del supervisore alla sola colpa grave – una prospettiva che ormai trova concordi diversi studiosi che si sono occupati dei rapporti tra i.a. e responsabilità penale⁴⁶. In altra sede, alla quale rinviemo, abbiamo tentato di formulare una possibile norma in questo senso, che tiene conto dei fattori che più possono incidere

⁴⁴ Per alcuni rilievi critici al criterio di delega previsto *sub art. 24, c. 5, lett. b)*, v. diffusamente B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit., p. 750 ss.

⁴⁵ Sul rischio di una frattura strutturale tra *obbligo di controllo* e *potere di controllo* v. B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit., p. 508 ss.

⁴⁶ V., in particolare, A. FIORELLA, *Responsabilità penale dei Tutor e dominabilità dell’Intelligenza Artificiale. Rischio permesso e limiti di autonomia dell’Intelligenza Artificiale*, in R. GIORDANO E AL. (a cura di), *Il diritto nell’era digitale. Persona, mercato, amministrazione, giustizia*, Giuffrè, 2022, pp. 662-663; nel settore delle macchine a guida autonoma v. M. LANZI, *Self-driving cars e responsabilità penale*, cit., p. 198 ss.; nel settore della *corporate governance* v. A. MANGIONE, *Intelligenza artificiale, attività d’impresa e diritto penale*, cit., p. 402.

sulla capacità del supervisore di conformarsi alle regole cautelari che disciplinano la sorveglianza dei sistemi di i.a.⁴⁷.

Ammettiamo, d'altra parte, di non essere del tutto convinti della necessità, quantomeno ad oggi, di una simile soluzione, nella misura in cui una limitazione della colpa *ad hoc*, di cui possano beneficiare soltanto i supervisori dei sistemi di i.a., introdurrebbe nell'ordinamento penale una disparità di trattamento della cui ragionevolezza si potrebbe opinare⁴⁸.

Piuttosto, una riduzione del rischio di eccessiva esposizione penale per il supervisore potrebbe derivare, in maniera a nostro avviso più equilibrata, dall'introduzione di una rigida separazione di "competenze" tra agente umano e algoritmo, che consenta al primo di *fare affidamento sull'ordinario funzionamento del sistema di i.a.* Tale soluzione, tuttavia, necessiterebbe di un approccio settoriale, che identifichi le applicazioni dell'intelligenza artificiale che – per la loro affidabilità, per il tipo di interazione i.a.-essere umano, e per i beni giuridici coinvolti – consentono di introdurre delle forme di affidamento. Non è dunque, di certo, in applicazione di una delega legislativa avente obiettivi *generali* che una simile operazione selettiva può essere effettuata.

8.4. La medesima lett. c) dell'art. 24, c. 5, delega poi il Governo alla precisazione dei criteri di imputazione della responsabilità "amministrativa degli enti", per gli "illeciti inerenti a sistemi di intelligenza artificiale". Dato il contesto, sembrerebbe di potersi ritenere che il riferimento sia alla responsabilità degli enti *ex d.lgs. 231/2001*. Gli indici che dovrebbero indurre a ritenere che l'intento della delega sia quello di una *limitazione* della responsabilità sono quelli già menzionati nel precedente paragrafo: il termine "precisazione" e il riferimento al "livello effettivo di controllo".

A ben guardare, tuttavia, non pare che siano rinvenibili delle esigenze di limitazione della responsabilità da reato degli enti. È piuttosto vero il contrario: vi sarebbe, in effetti, la necessità di *estendere* l'elenco dei reati-presupposto, per comprendervi quantomeno i reati di omicidio e lesioni colpose commessi nell'ambito dell'attività produttiva – un'esigenza che era già emersa con riferimento alla casistica "tradizionale" del danno da prodotto⁴⁹ –, e per includere altresì le nuove fattispecie di pericolo introdotte in attuazione della delega (v. *supra*, par. 8.2.).

Va infatti osservato che spesso, sia sul versante della *produzione* dei sistemi di i.a., sia sul versante del loro *impiego*, è il soggetto collettivo, più che la persona fisica, il reale centro degli interessi coinvolti nella commissione del reato, e l'espansione dell'elenco

⁴⁷ B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit., p. 730.

⁴⁸ Per un'illustrazione più ampia delle ragioni a fondamento di tale posizione v. B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit., p. 722 ss.

⁴⁹ Cfr. a tal proposito A. BERNARDI, *La responsabilità da prodotto nel sistema italiano: profili sanzionatori*, in *Riv. trim. dir. pen. ec.*, 1-2, 2003, p. 11, che rilevava criticamente come il d.lgs. 231/2001 non potesse applicarsi ai reati di omicidio colposo e lesioni colpose commessi con violazione delle norme sulla tutela della salute e della sicurezza del lavoro e ai reati ambientali. Sebbene tali fattispecie siano state successivamente inserite nell'elenco dei reati-presupposto, resta ferma l'inapplicabilità della responsabilità *ex d.lgs. 231/2001* alle fattispecie che riguardano la messa in commercio di prodotti pericolosi o lesivi.

dei *predicate crimes* è un primo passo ineludibile – anche se, va detto, forse non sufficiente⁵⁰ – per rendere applicabile il d.lgs. 231/2001 alla nuova criminalità “da intelligenza artificiale”.

È difficile, tuttavia, che una simile operazione possa essere effettuata, in attuazione della lett. c) dell’art. 24, c. 5, l. 132/2025, senza che si sfoci in un *eccesso di delega*. O meglio, delle due l’una: o si ritiene che il criterio previsto dalla delega imponga effettivamente un *intervento delimitativo* della responsabilità degli enti, e allora un’estensione dell’elenco dei reati-presupposto contenuto nel d.lgs. 231/2001 non sarebbe ammissibile; oppure si ritiene che la delega non fornisca *alcun criterio politico-criminale* al Governo, il che dovrebbe ritenersi inequivocabilmente incompatibile con il principio di riserva di legge penale, oltre che, evidentemente, con l’art. 76 Cost.

8.5. Infine, la lett. f) prevede una revisione “complessiva del sistema”, in conformità ai principi già enunciati: anche in questo caso, un’indeterminatezza che si pone in tensione con il principio di riserva di legge, e che potrebbe aprire la strada ai più svariati interventi legislativi.

9. La sensazione complessiva che si ha, leggendo le disposizioni di rilievo penalistico contenute nella legge 132/2025, è che il legislatore abbia rinviato ad un momento successivo – all’attuazione delle deleghe da parte del Governo – la risoluzione di alcune delle questioni più spinose inerenti all’imputazione della responsabilità penale per i c.d. *AI-crimes*. Se si escludono le nuove fattispecie in materia di *deepfakes* e di diritto d’autore, l’intervento diretto della legge è infatti limitato alla facile “arma” delle aggravanti – a conferma di una tendenza ormai ampiamente affermatasi nella legislazione penale contemporanea, che sempre più spesso vede nelle aggravanti uno strumento poco oneroso per segnalare ai consociati una presa in carico simbolica delle più svariate esigenze di tutela.

Sarà dunque il Governo a dover prendere posizione su alcuni degli interrogativi più complessi che riguardano i rapporti tra i.a. e responsabilità penale:

- innanzitutto, in quali forme potrà concretizzarsi un’anticipazione della tutela penale – anticipazione a nostro avviso indispensabile, affinché la crisi del diritto penale di evento-danno, determinata dall’imprevedibilità dell’intelligenza artificiale, non si traduca in una sostanziale deresponsabilizzazione dei produttori dei sistemi di i.a.;
- in secondo luogo, come garantire – attraverso una limitazione della responsabilità penale – che la persona incaricata della supervisione

⁵⁰ Laddove l’imprevedibilità dell’intelligenza artificiale impedisca di muovere un rimprovero colpevole all’operatore umano, il d.lgs. 231/2001 si rivelerà infatti inapplicabile, stante la portata limitata del principio di autonomia sancito dall’art. 8; sulle potenzialità e i limiti della responsabilità “da reato” degli enti, nel settore dell’intelligenza artificiale, sia consentito il rinvio a B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit., p. 737 ss.

dell'intelligenza artificiale non si trasformi in un capro espiatorio, destinato a rispondere di *default* per tutti gli eventi lesivi derivanti dall'impiego del dispositivo;

- infine, quale ruolo è chiamato a rivestire, in questo settore, il sistema della responsabilità da reato degli enti, specialmente in un contesto in cui l'AI Act prevede già un apparato di sanzioni amministrative – evidentemente riconducibili alla *matière pénale*⁵¹ – destinato ad applicarsi ai produttori e agli utilizzatori professionali dei sistemi di i.a. che non rispettino le disposizioni contenute nel Regolamento. Si noti, a tal proposito, che, oltre alla delega in materia penale, l'art. 24 della legge 132/2025 prevede, al comma primo, una delega finalizzata all'«adeguamento della normativa nazionale al regolamento (UE) 2024/1689», comprensiva dell'«adeguamento del quadro sanzionatorio».

Il rapporto tra sanzioni penali, sanzioni *ex d.lgs.* 231/2001, e sanzioni amministrative “para-penali” previste dall'AI Act è uno dei profili sui quali, in vista dell'attuazione della delega, varrebbe la pena avviare un'attenta riflessione – così da non ritrovarci, ancora una volta, con l'ennesimo doppio binario sanzionatorio in odore di incostituzionalità. Se in relazione a specifiche forme di offesa può senz'altro rendersi opportuno un intervento penalistico, è infatti indispensabile individuare meccanismi di coordinamento che scongiurino la duplicazione dei procedimenti in relazione all'*idem factum*⁵².

Occorre evitare, insomma, che da un rischio di *deresponsabilizzazione* si passi ad un *carico punitivo sproporzionato* a carico dei produttori e degli utilizzatori dei sistemi di i.a.⁵³.

⁵¹ V., ad esempio, il par. 3 dell'art. 99 AI Act, che, in merito alla violazione «del divieto delle pratiche di IA di cui all'articolo 5», prevede «sanzioni amministrative pecuniarie fino a 35 000 000 EUR o, se l'autore del reato è un'impresa, fino al 7 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore».

⁵² Sul recente ritorno ad una valorizzazione del *volet* processuale del principio del *ne bis in idem*, ad opera della Corte costituzionale, v. N. RECCHIA, *L'ennesima stagione del ne bis in idem nel costituzionalismo multilivello: la riaffermazione del suo ubi consistam processuale contro ogni riduzionismo sostanziale*, in *Riv. it. dir. proc. pen.*, 4, 2022, p. 1693 ss.

⁵³ Per alcune proposte di intervento penale *de iure condendo* – prese in considerazione anche alla luce del testo del d.d.l. 1146/2024, all'origine della legge in commento – sia consentito, ancora una volta, il rinvio a B. FRAGASSO, [Intelligenza artificiale e responsabilità penale](#), cit., p. 688 ss.

**PER LA CORTE PENALE INTERNAZIONALE
L'ITALIA HA VIOLATO GLI OBBLIGHI DI COOPERAZIONE
PER VIA DELLA MANCATA CONSEGNA DEL LIBICO ALMASRI
ALL'AIA**

International Criminal Court, Pre-Trial Chamber I, 17 ottobre 2025

di Maria Crippa

1. Pochi giorni dopo la [decisione della Camera dei deputati di negare l'autorizzazione a procedere](#) nei confronti del Ministro della giustizia Carlo Nordio, del Ministro dell'interno Matteo Piantedosi e del Sottosegretario di Stato alla Presidenza del Consiglio dei ministri Alfredo Mantovano, la Camera preliminare I della Corte penale internazionale (Cpi) ha ritenuto sussistente la violazione da parte dell'Italia degli obblighi internazionali di cooperazione sanciti dall'art. 87(7) Statuto di Roma (qui il testo del [provvedimento](#)). La Cpi ha invece rimandato ad un secondo momento la decisione sul deferimento dello Stato all'Assemblea degli Stati parte (Assembly of States Parties, ASP) ovvero al Consiglio di Sicurezza delle Nazioni Unite (United Nations Security Council, UNSC), sempre ai sensi dell'art. 87(7) dello Statuto. La decisione si inserisce nel procedimento avviato nei confronti dell'Italia a seguito della mancata consegna di Osama Elmasry Njeem (anche noto come Almasri), arrestato a Torino il 19 gennaio 2025, in esecuzione di una *red notice* dell'Interpol e del [mandato di arresto emesso dalla Cpi](#) il giorno precedente. La Camera preliminare I della Cpi aveva infatti ritenuto sussistenti "ragionevoli motivi per ritenere", secondo lo standard probatorio imposto dall'art. 58(1) Statuto di Roma, che Almasri avesse commesso [crimini di guerra e crimini contro l'umanità](#) a partire dal 15 febbraio 2015 nel centro di detenzione di Mitiga, vicino a Tripoli, all'epoca dei fatti sotto il suo controllo. Il 21 gennaio la Corte d'Appello di Roma, in accoglimento della richiesta del Procuratore Generale, aveva dichiarato [non luogo a provvedere sull'arresto di Almasri in quanto eseguito 'irritualmente'](#), in assenza di preve interlocuzioni con il Ministro della Giustizia (sui profili di criticità della decisione si veda, *ex multis*, [qui](#), [qui](#), [qui](#), [qui](#) e [qui](#)). Almasri era stato, quindi, [immediatamente rimesso in libertà e rimpatriato, in quanto soggetto pericoloso](#).

2. Il 17 febbraio 2025 [la Camera preliminare aveva invitato l'Italia a depositare le proprie osservazioni](#) sulla mancata consegna di Almasri alla Corte, così attivando le consultazioni previste dalla Regola 109 delle Regole della Corte. Nel proprio provvedimento del 21 febbraio, [il Procuratore della Cpi aveva chiesto alla Camera preliminare I di dichiarare la violazione da parte dell'Italia degli obblighi di cooperazione ai sensi dell'art. 87\(7\) Statuto di Roma](#), per la mancata esecuzione della richiesta sia di arresto e consegna di Almasri, sia di perquisizione e sequestro dei materiali trovati in suo possesso. Il 6 maggio, a seguito di due proroghe consecutive del

termine per il deposito (inizialmente previsto per il 17 marzo), l'Italia aveva presentato alla Cpi le proprie osservazioni. A queste erano seguite le osservazioni conclusive del Procuratore (il 25 giugno) e quelle di replica dell'Italia (il 28 luglio).

3. Merita ricordare che il procedimento previsto dall'art. 87(7) Statuto di Roma viene instaurato a seguito di una presunta violazione degli obblighi di cooperazione imposti agli Stati parte dagli artt. 86-102 Statuto di Roma. Gli Stati parte allo Statuto di Roma hanno, infatti, un obbligo generale di cooperazione con la Corte, che può avanzare richieste di consegna (artt. 89-90 Statuto di Roma), arresto e consegna (art. 91 Statuto di Roma), arresto provvisorio in casi di urgenza (art. 92 Statuto di Roma) e altre forme di cooperazione (art. 93 Statuto di Roma). In caso di mancato ottemperamento a tali richieste, la Cpi può dichiarare la violazione degli obblighi imposti dallo Statuto di Roma. Il giudizio *ex art. 87(7) Statuto di Roma* si compone di due condizioni cumulative: i) lo Stato deve avere mancato di ottemperare alla richiesta della Cpi; e ii) la mancata cooperazione deve essere sufficientemente grave da avere impedito alla Corte l'esercizio delle proprie funzioni e dei propri poteri. A fronte della condanna dello Stato per la violazione degli obblighi di cooperazione, la Cpi può quindi decidere se deferire la questione all'ASP ovvero all'UNSC, laddove la giurisdizione della Cpi sia stata attivata mediante *referral* di tale organismo al Procuratore della Cpi, come nel caso della [Libia](#).

4. In passato, la Cpi si è già confrontata con altri casi di mancata cooperazione nell'esecuzione delle richieste di consegna di soggetti attinti da mandato di arresto della Corte. Un esempio particolarmente significativo è costituito dalle numerose decisioni di condanna nei confronti di diversi Stati (tra i quali [Giordania](#), [Sudafrica](#), [Ciad](#) e [Malawi](#)) che si erano rifiutati di arrestare e consegnare l'ex presidente sudanese Omar al-Bashir, oggetto di due mandati di arresto per crimini contro l'umanità, crimini di guerra e genocidio. Più di recente, [la Mongolia è stata ritenuta responsabile](#) per il mancato arresto e la mancata consegna del presidente russo Vladimir Putin, sul quale pende un mandato di arresto della Cpi per crimini di guerra, e lo stesso è accaduto all'[Ungheria](#) nei confronti del primo ministro israeliano Benjamin Netanyahu, ricercato dalla Corte per crimini contro l'umanità e crimini di guerra.

5. La decisione della Camera preliminare I sulla violazione degli obblighi di cooperazione. – I giudici hanno ritenuto all'unanimità la condotta del governo italiano in violazione degli obblighi di cooperazione sanciti dall'art. 87(7) Statuto di Roma. La Camera preliminare ha, infatti, ricordato che l'Italia aveva ricevuto la richiesta di arresto provvisorio di Almasri già il 18 gennaio, attraverso i canali diplomatici designati. Nonostante la tempestiva esecuzione del mandato di arresto, la rimessione in libertà e il rimpatrio di Almasri avevano impedito alla Cpi l'esercizio del potere di assicurare la presenza del sospettato di fronte alla Corte, condizione peraltro necessaria per la prosecuzione del procedimento, quantomeno dopo la fase della conferma delle accuse (artt. 61 e 63 Statuto di Roma). L'Italia aveva poi omesso le necessarie consultazioni

imposte dall'art. 97 Statuto di Roma nell'ipotesi di ostacoli all'esecuzione delle richieste della Corte, peraltro richieste dal Registro della Cpi tra il 19 e il 21 gennaio.

6. La Camera preliminare I ha quindi sottolineato il carattere contraddittorio delle ragioni addotte dall'Italia nelle proprie osservazioni. Quanto alla mancata previa interlocuzione con il Ministro della giustizia, i giudici hanno evidenziato che, ai sensi dell'art. 88 Statuto di Roma, gli Stati hanno la responsabilità di adottare procedure interne che consentano la cooperazione con la Cpi. Inoltre, la richiesta di arresto provvisorio era stata trasmessa ai canali diplomatici individuati dallo stesso Stato italiano e, ad ogni modo, inviata al Ministro della giustizia alla prima occasione possibile.

7. L'Italia aveva poi riferito di avere ricevuto una concorrente richiesta di estradizione dalla Libia nei confronti di Almasri e per le stesse condotte oggetto del mandato di arresto della Cpi. Sul punto, i giudici hanno ricordato che in caso di concorrenti richieste di estradizione, anche da parte di ordinamenti terzi allo Statuto di Roma, lo Stato è tenuto a notificare tempestivamente la Cpi (art. 90 Statuto di Roma). Al contrario, il governo italiano aveva sollevato tale evenienza solo il 7 maggio 2025, venendo meno anche in questo caso all'obbligo di consultazione con la Corte. Come notato dal collegio, inoltre, Almasri non era stato consegnato alle autorità libiche a seguito di una procedura di estradizione, ma aveva fatto ritorno in Libia in libertà.

8. Quanto ai presunti errori contenuti nel mandato di arresto, la Camera preliminare ha rilevato che si trattava di mere difformità tipografiche tra dispositivo e parte motiva, presenti nella prima versione del provvedimento ed emendate il 24 gennaio 2025. Non si trattava, invece, di errori sostanziali relativi ai crimini oggetto di imputazione né alla responsabilità individuale di Almasri, tali da inficiare la validità del mandato di arresto. La circostanza, poi, che vi fosse una opinione dissenziente al mandato, alla luce del fatto che la Cpi può prendere determinazioni a maggioranza, non poteva costituire una valida ragione per l'Italia per contestare la legittimità della decisione.

9. Da ultimo, i giudici hanno evidenziato la contraddittorietà della decisione di espellere Almasri in Libia, stante la sua particolare pericolosità per la commissione di gravi crimini internazionali proprio nel paese. In questo senso, l'Italia aveva omesso di fornire alla Corte informazioni tempestive su tale decisione.

10. La Camera preliminare I ha, a maggioranza, posticipato la decisione sul deferimento dell'Italia all'ASP ovvero all'UNSC, invitando lo Stato a presentare entro il 31 ottobre 2025 informazioni circa l'esistenza e l'impatto di eventuali procedimenti interni. La Camera preliminare ha in primo luogo ricordato il carattere pienamente discrezionale della decisione, che costituisce un rimedio volto a rafforzare l'effettività del regime di cooperazione con la Cpi. Nel caso di specie, la maggioranza del collegio ha richiamato il procedimento instaurato di fronte al Tribunale dei Ministri nei confronti

dei membri del governo sopra indicati e della Presidente del Consiglio Giorgia Meloni. La Camera preliminare ha sul punto ricordato la propria [decisione di non deferire il Sudafrica all'ASP o all'UNSC](#), nonostante la mancata consegna di al-Bashir, alla luce di una pronuncia della Suprema Corte d'Appello che sanciva la violazione da parte del governo degli obblighi di cooperazione con la Cpi.

11. Inoltre, i giudici hanno evidenziato la sussistenza di condizioni che, lungi dal giustificare la condotta dell'Italia, potevano essere tuttavia rilevanti nella determinazione dell'utilità di un suo deferimento alle istituzioni internazionali, quali il carattere repentino e complesso della situazione, la confusione creata dall'intervento di diversi organi e la circostanza che si trattava del primo caso di cooperazione con la Cpi.

12. Sul punto, la giudice Maria del Socorro Flores Liera ha depositato [una opinione parzialmente dissenziente](#), ritenendo insussistenti ragioni idonee a ritardare il deferimento dell'Italia all'ASP. La giudice ha rigettato l'interpretazione "estremamente ampia" del collegio circa la natura discrezionale del provvedimento e ritenuto sussistenti nel caso di specie tutte le condizioni previste dall'art. 87(7) Statuto di Roma. In particolare, la gravità della condotta dell'Italia doveva desumersi dalle conseguenze della stessa sul procedimento instaurato di fronte alla Cpi e, in senso più ampio, sul mandato della Corte di porre fine alle impunità per i più gravi crimini di interesse della comunità internazionale. La serietà delle violazioni imputate allo Stato italiano era, inoltre, evidente dalla mancata assunzione di responsabilità e volontà a cooperare con la Cpi. Da ultimo, la giudice dissenziente ha evidenziato come una decisione di non deferire la questione all'ASP si porrebbe in contraddizione con la giurisprudenza della Cpi e con gli obiettivi del regime di cooperazione imposto dallo Statuto di Roma. Il deferimento all'ASP ovvero all'UNSC costituirebbe, invece, l'unico strumento appropriato per promuovere la cooperazione dell'Italia e, più in generale, degli Stati con la Cpi.

13. La decisione in esame rappresenta uno snodo fondamentale nel procedimento aperto nei confronti dell'Italia per la violazione degli obblighi di cooperazione con la Cpi. Se, da un lato, la Camera preliminare si è espressa all'unanimità in termini molto netti e severi sulla mancata consegna di Almasri alla Corte, la decisione di rinviare il deferimento all'ASP ovvero all'UNSC, dando ancora una volta all'Italia la possibilità di presentare osservazioni in proposito, solleva qualche dubbio. A margine di considerazioni circa [l'assenza di rimedi effettivi per le ipotesi di mancata cooperazione con la Cpi](#), in un momento storico di particolare messa in discussione della Corte, ci si limita a ricordare che nell'ordinamento italiano non sono, allo stato, aperti procedimenti interni volti a valutare le eventuali responsabilità individuali per la vicenda Almasri. Basti sul punto richiamare la citata decisione della Camera dei deputati di negare l'autorizzazione a procedere nei confronti del Ministro della giustizia, del Ministro dell'interno e del Sottosegretario di Stato alla Presidenza del Consiglio dei ministri, diversamente dalle conclusioni della [relazione del Tribunale dei Ministri ai](#)

10/2025

[sensi dell'art. 96 Cost.](#) Proprio la mancanza di rimedi interni esperibili ha fondato il [ricorso di una delle vittime del generale libico](#) .

Editore

ASSOCIAZIONE
**"PROGETTO GIUSTIZIA
PENALE"**