# Le modifiche al Codice penale introdotte dalla normativa nazionale in materia di intelligenza artificiale (L. 132/2025)

*di Beatrice Scialla - pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale, 25 marzo 2026*

*La nuova legge nazionale sull'intelligenza artificiale (legge 23 settembre 2025, n. 132) introduce rilevanti modifiche al Codice penale: prevede aggravanti – comuni e speciali – per i reati commessi mediante l'impiego di sistemi di A.I. e introduce una fattispecie autonoma di reato, l'articolo 612-quater c.p. Quest'ultimo sanziona l'illecita diffusione di contenuti generati o alterati tramite intelligenza artificiale, sollevando significative problematiche sia a livello interpretativo che di sistematica codicistica.*

L'atteggiamento attendista degli Stati membri in merito all'adozione di normative in materia di A.I. è stato bruscamente interrotto dall'Italia, primo Stato a proporre una legge nazionale in materia, in vigore dal 10 ottobre 2025 (M. Azzella, M. Monaco, Intelligenza Artificiale: la sfida del Governo).

A differenza dell'A.I. Act che introduce una disciplina orizzontale (M. Ebers, Truly Risk-based Regulation of Artificial Intelligenge How to Implement the EU's AI Act; B. Marchetti, La regolazione europea del mercato dell'intelligenza artificiale), la legge italiana sull'intelligenza artificiale sposa un'**impostazione settoriale**, introducendo dapprima dei principi valevoli per tutti gli ambiti, contenuti nel Capo I, proseguendo poi con disposizioni specifiche, tarate sui vari settori di interesse.

Una delle principali novità della legge è la previsione di un apposito Capo V, dedicato alle disposizioni penali in materia di A.I. Occorre ricordare che già l'A.I. Act ha inserito alcune previsioni di rilievo penalistico, lasciando ampi spazi di autonomia agli Stati membri. Oltre ai sistemi vietati ai sensi dell'articolo 5 del regolamento europeo – tra cui quelli di *risk assessment,* di polizia predittiva nonché di identificazione biometrica in tempo reale – utilizzati soprattutto nel corso delle indagini, l'Allegato III ha individuato alcuni sistemi ad alto rischio di rilevanza penalistica. Il paragrafo 6 del medesimo Allegato è dedicato alle attività di contrasto (*law enforcement*), «nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso». Con tale inciso, l'A.I. Act ha inteso chiarire che la sola inclusione nell'Allegato III non comporta una automatica armonizzazione delle discipline dei singoli ordinamenti, che conservano autonomia nella valutazione della legittimità di utilizzo degli strumenti di A.I. (S. Quattrocolo, Intelligenza artificiale e processo penale: le novità dell'AI Act).

Ancor prima dell'A.I. Act, nel 2018, la Commissione europea per l'efficacia della giustizia (CEPEJ) ha adottato una Carta etica europea sull'utilizzo dell'A.I. nei sistemi giudiziari e negli ambiti connessi. È in questo contestoche si inseriscono le novità introdotte dalla legge italiana (A. Giannini, Intelligenza artificiale, *human oversight*e responsabilità penale: prove d'impatto a livello europeo), le quali appaiono in linea con i principi sanciti a livello europeo, pur non traducendosi in un

articolato normativo in grado di contrastare tutti i potenziali rischi derivanti dall'uso dell'A.I. (S. De Flammineis, Fattispecie penali nel contesto dell'intelligenza artificiale. Lo spunto del D.D.L. 1146/2024).

**L'articolo 26, comma 1 della legge sull'A.I. prevede un triplice intervento sul Codice penale, volto a punire reati commessi con l'ausilio di sistemi di A.I.** e a scongiurarne l'utilizzo per fini criminosi, visti gli elevati trattamenti sanzionatori ivi previsti. In particolare, è prevista la modifica dell'articolo 61 c.p. in materia di aggravanti comuni, l'inasprimento del trattamento sanzionatorio per il reato di cui all'art. 294 c.p. se l'inganno, che ne costituisce condotta tipica, è realizzato mediante l'impiego di sistemi di A.I., ed infine l'introduzione di una nuova fattispecie di reato, l'art 612-quater c.p.

Sotto il primo profilo, viene aggiunto all'art 61 c.p. il nuovo comma 11-*undecies*, il quale configura come aggravante comune la commissione di un reato mediante l'impiego di sistemi di A.I., qualora essi – per natura o modalità di utilizzo – abbiano costituito un mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, oppure aggravato le conseguenze del reato. Dalla lettera della legge si evince che per l'addebito dell'aggravante non è sufficiente il mero impiego dei sistemi di A.I., come previsto per le circostanze speciali, ma è richiesto un *quid pluris*, riscontrabile nell'impiego dell'A.I. in qualità di **mezzo subdolo**, **in grado di acuire l'offesa** ostacolando la difesa ovvero aggravando le conseguenze del reato.

**La nuova legge interviene anche sul delitto di attentati contro i diritti politici del cittadino, previsto dall'art. 294 c.p., innalzando la pena** – ricompresa in una ampia cornice edittale tra due e sei anni – **qualora l'inganno sia realizzato mediante sistemi di A.I.** In tal caso, l'utilizzo dell'A.I. integra una aggravante speciale, che detta un trattamento sanzionatorio più severo del reato base. Si presume, cioè, che il solo impiego dell'A.I. sia sufficiente ad aggravare il disvalore dell'inganno che impedisce l'esercizio di un diritto politico, ovvero determina taluno a esercitarlo in senso difforme alla sua volontà. La *ratio* è da ricercare nella crescente attenzione verso fenomeni di manipolazione dei diritti politici – primo tra tutti il diritto di voto – mediante le nuove tecnologie, anche alla luce di pregresse esperienze, come il noto caso Cambridge Analytica.

Di particolare rilievo è poi la **creazione di una nuova fattispecie di reato all'art. 612-quater c.p.**, rubricato "Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale". La nuova ipotesi criminosa punisce con la reclusione da uno a cinque anni **chiunque cagioni un danno ingiusto mediante la cessione, la pubblicazione o la diffusione di immagini, video, o voci falsificati o alterati mediante l'impiego di intelligenza artificiale, senza il consenso della persona interessata, purché tali contenuti siano idonei ad indurre in inganno sulla loro genuinità**.

La norma prende di mira i c.d. ***deepfake* non consensuali**, ovvero falsi digitali altamente realistici diffusi senza consenso, (B. Zoina, Informazione e disinformazione nell'era dell'IA) e si inserisce in un *trend* – già inaugurato con il disegno di legge spagnolo sull'intelligenza artificiale – che mira a contrastare la diffusione di contenuti digitali falsi che siano in grado di ingannare circa la loro natura, imponendo un severo trattamento sanzionatorio.

Quanto alla procedibilità del reato, esso è perseguibile a querela, salvo il fatto non sia commesso insieme ad altro reato per cui si debba procedere d'ufficio o nei confronti di persona incapace o una pubblica autorità a causa delle funzioni esercitate.

L'onere probatorio a carico dell'accusa risulta assai gravoso. Sarà anzitutto necessario dimostrare una delle condotte tipiche (cessione, pubblicazione o diffusione indebita), servendosi dei criteri ermeneutici utilizzati in altre fattispecie penali aventi ad oggetto la medesima condotta, come la diffusione di riprese e registrazioni fraudolente ai sensi dell'art 617-septies c.p. o il reato di pedopornografia ex art. 600-ter c.p. Dopodiché, trattandosi di un reato di danno, occorrerà dimostrare che una delle condotte summenzionate abbia causato un danno ingiusto ad una persona fisica, provando quindi il nesso causale che unisce la condotta e il danno (S. Quattrocolo, Intelligenza artificiale e processo penale: le novità dell'AI Act). Ciò non è ancora sufficiente, poiché sarà necessario provare anche l'effettiva alterazione del contenuto tramite A.I. – particolarmente difficile da ricostruire *ex post* – nonché l'idoneità del contenuto manipolato a indurre il destinatario in errore (Osservatorio compliance 231, Nuove fattispecie penali introdotte dalla L. 132/2025: 612 quater c.p. e relativa circostanza aggravante ex art 61 n.11 decies, c.p.).

**La fattispecie dal gravoso onere probatorio e dai contorni vaghi ha sollevato una serie di questioni.**

Innanzitutto, circa i profili di **indeterminatezza**, non è specificata la nozione di danno accolta dalla fattispecie. Tuttavia, visto che tutti i beni giuridici protetti – l'integrità morale, la reputazione e la libertà sessuale – sono di primaria importanza per il nostro ordinamento, è presumibile che sia incluso tra i danni punibili anche quello non patrimoniale.

Anche la valutazione dell'idoneità del contenuto a trarre in inganno circa la propria genuinità solleva alcune **questioni interpretative**. L'apparente genuinità del contenuto va considerata in relazione all'oggettiva verosimiglianza del *deepfake* rispetto al contenuto originale a prescindere dalle caratteristiche del destinatario? Oppure deve essere valutata in funzione della capacità del soggetto di discernere un contenuto veritiero da uno falso?

Il timore è di aver costruito una fattispecie eccessivamente aperta alla discrezionalità del giudice, in tensione con il principio di determinatezza ed espressione di una

risposta sanzionatoria mossa dall'allarme sociale più che dall'effettiva offensività delle condotte.

Pur essendo condivisibile l'insidiosità dei sistemi di A.I., occorre evitare una criminalizzazione eccessiva e diffusa, dettata esclusivamente dal timore di tecnologie ancora in parte sconosciute. Una simile deriva comporterebbe due conseguenze dannose. In primo luogo, limiterebbe aprioristicamente – e talvolta ingiustificatamente – l'impiego dell'A.I. per paura, invece di orientarne l'uso a finalità virtuose. In secondo luogo, risponderebbe a logiche di populismo penale, rischiando un inasprimento sanzionatorio sproporzionato in grado di alterare l'equilibrio sistematico del Codice penale.