UNIVERSITÀ DEGLI STUDI DI MILANO

Facoltà di Giurisprudenza
Pubblicazioni del Dipartimento di Diritto pubblico italiano e sovranazionale

COMMENTARIO TEMATICO DEL REGOLAMENTO (UE) 2024/1689 E DELLA LEGGE ITALIANA 23 SETTEMBRE 2025, N. 132

a cura di

MARILISA D'AMICO, FRANCISCO BALAGUER CALLEJÓN,
AUGUSTO AGUILAR CALAHORRO, PAOLO GAMBATESA, SARA DI GIOVANNI

G. Giappichelli Editore

UNIVERSITÀ DEGLI STUDI DI MILANO

Facoltà di Giurisprudenza
Pubblicazioni del Dipartimento di Diritto pubblico italiano e sovranazionale

Studi di diritto pubblico

126

La Collana “Pubblicazioni del Dipartimento di Diritto pubblico italiano e sovranazionale” dell’Università degli Studi di Milano raccoglie monografie e altri risultati inediti di ricerche, individuali e collettive, di studiosi che svolgono attività di studio e ricerca nel Dipartimento.
Essa comprende Studi di Diritto costituzionale, di Diritto amministrativo, di Diritto internazionale ed europeo, di Diritto processuale civile, di Diritto comparato, di Storia del diritto, di Politica economica.
La qualità scientifica delle pubblicazioni è assicurata da una procedura di c.d. double blind peer review ad opera di revisori esterni.

COMMENTARIO TEMATICO DEL REGOLAMENTO (UE) 2024/1689 E DELLA LEGGE ITALIANA 23 SETTEMBRE 2025, N. 132

a cura di

MARILISA D'AMICO, FRANCISCO BALAGUER CALLEJÓN,
AUGUSTO AGUILAR CALAHORRO, PAOLO GAMBATESA, SARA DI GIOVANNI

G. Giappichelli Editore

VIA PO, 21 - TEL. 011-81.53.111
http://www.giappichelli.it

ISBN/EAN 979-12-211-1875-9
ISBN/EAN 979-12-211-6631-6 (ebook-pdf)
ISBN/EAN 979-12-211-6722-1 (ebook-epub)

Il volume è edito con risorse del PRIN 2022 CUP G53D23002160006 - Finanziato dall'unione europea - Next Generation EU Misura M4C2 – Investimento 1.1.

Finanziato dall'Unione europea NextGenerationEU
MUR
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
UNIVERSITÀ DEGLI STUDI DI MILANO

Stampa: Stampatre s.r.l. - Torino

INDICE

pag.

pag.

pag.

SEZIONE II
DIRITTI E GARANZIE FONDAMENTALI NEI SISTEMI VIETATI

pag.

pag.

pag.

SEZIONE III
SISTEMI DI INTELLIGENZA ARTIFICIALE AD ALTO RISCHIO

A) *Classificazione*

pag.

pag.

pag.

pag.

pag.

pag.

SEZIONE VI
SORVEGLIANZA, CONTROLLO E SANZIONI

CAPITOLO XXX
MONITORAGGIO, APPLICAZIONE E GARANZIE, SANZIONI
Commento agli artt. 72-94 e 99-101

CAPITOLO XXXI
IL RUOLO DELLA *SOFT LAW* NELL'ATTUAZIONE DELL'AI ACT
Commento agli artt. 95 e 96

pag.

PARTE II
LA LEGGE 23 SETTEMBRE 2025, N. 132

pag.

pag.

pag.

pag.

ELENCO DEGLI AUTORI E DELLE AUTRICI

Giulia Agrati, Dottoressa di ricerca in Diritto dell'Unione europea, Università degli Studi di Milano.

Augusto Aguilar Calahorro, Profesor Titular de Derecho Constitucional, Universidad de Granada.

Ilaria Anrò, Professoressa Associata di Diritto dell'Unione europea, Università degli Studi di Milano.

Giuseppe Arconzo, Professore Ordinario di Diritto costituzionale, Università degli Studi di Milano.

Miguel José Arjona Sánchez, Profesor Ayudante Doctor de Derecho Constitucional, Universidad de Granada.

Francisco Balaguer Callejón, Catedrático de Derecho Constitucional, Universidad de Granada.

Michael Bianchi, Dottorando di ricerca in Diritto costituzionale, Università degli Studi di Milano.

Camilla Burelli, Ricercatrice a tempo determinato in Diritto dell'Unione europea, Università degli Studi di Milano.

Gregorio Cámara Villar, Catedrático de Derecho Constitucional, Universidad de Granada.

Stefano Catalano, Professore Ordinario di Diritto costituzionale, Università degli Studi di Verona.

Marilisa D'Amico, Professoressa Ordinaria di Diritto costituzionale, Università degli Studi di Milano.

Sara Di Giovanni, Titolare di incarico di ricerca in Diritto costituzionale, Università degli Studi di Milano.

Nannerel Fiano, Ricercatrice a tempo determinato in Diritto costituzionale, Università degli Studi di Milano.

Emma Fidenzi, Dottoranda di ricerca in Diritto costituzionale, Università degli Studi di Milano.

Beatrice Fragasso, Assegnista di ricerca in Diritto penale, Università degli Studi di Milano.

Adoración Galera Victoria, Profesora Titular de Derecho Constitucional, Universidad de Granada.

Paolo Gambatesa, Assegnista di ricerca in Diritto costituzionale, Università degli Studi di Milano.

Fabiola Giotto, Dottoressa in Giurisprudenza, Università degli Studi di Milano.

Lorenzo Grossi, Dottorando di ricerca in Diritto amministrativo, Università degli Studi di Milano.

Enrique José Guillén López, Catedrático de Derecho Constitucional, Universidad de Granada.

Rosa Iannaccone, Contrattista di ricerca in Diritto pubblico comparato, Università degli Studi di Sassari.

Alessandra Ingrao, Professoressa Associata di Diritto del lavoro, Università degli Studi di Milano.

Antonino La Lumia, Presidente dell'Ordine degli Avvocati di Milano.

Stefania Leone, Professoressa Associata di Diritto costituzionale, Università degli Studi di Milano.

Benedetta Liberali, Professoressa Associata di Diritto costituzionale, Università degli Studi di Milano.

Amalia Lozano España, Contratada Predoctoral de Derecho Constitucional, Universidad de Granada.

Marta Lucena Pérez, Contratada Predoctoral de Derecho Constitucional, Universidad de Granada.

Francesca Marinelli, Professoressa Associata di Diritto del Lavoro, Università degli Studi di Milano.

Luis Fernando Martínez Quevedo, Profesor de Derecho Constitucional, Universidad de Granada.

Costanza Nardocci, Professoressa Associata di Diritto costituzionale, Università degli Studi di Milano.

Giacomo Palombino, Investigador García-Pelayo, Centro de Estudios Políticos y Constitucionales, Madrid.

Niccolò Panigada, Titolare di incarico di ricerca in Diritto costituzionale, Università degli Studi di Milano.

Gaia Patarini, Dottoranda di ricerca in Diritto costituzionale, Università degli Studi di Milano.

Irene Pellizzone, Professoressa Associata di Diritto costituzionale, Università degli Studi di Milano.

Eloisa María Pérez Conchillo, Profesora Ayudante Doctora de Derecho Constitucional, Universidad de Granada.

Antonio Pérez Miras, Profesor Permanente Laboral de Derecho Constitutional, Universidad de Granada.

Elisa Pignanelli, Dottoranda di ricerca in Diritto costituzionale, Università degli Studi di Milano.

Juan Francisco Sánchez Barrilao, Catedrático de Derecho Constitucional, Universidad de Granada.

Cecilia Siccardi, Ricercatrice a tempo determinato in Diritto costituzionale, Università degli Studi di Milano.

Marta Annamaria Tamborini, Dottoranda di ricerca in Diritto costituzionale, Università degli Studi di Milano.

Pietro Villaschi, Ricercatore a tempo determinato in Diritto costituzionale, Università degli Studi di Milano.

CAPITOLO XVIII
LE DISPOSIZIONI PENALI: L'IA COME *INSTRUMENTUM SCELERIS*
Commento all'art. 26

Beatrice Fragasso

SOMMARIO: 1. Intelligenza artificiale e responsabilità penale: una premessa. – 2. La definizione di intelligenza artificiale come elemento normativo delle disposizioni penali (rinvio). – 3. La fattispecie di illecita diffusione di contenuti generati o manipolati artificialmente. – 4. La nuova fattispecie in materia di diritto d'autore. – 5. Le nuove circostanze aggravanti. – 6. Brevi cenni ai criteri di delega in materia penale contenuti nell'art. 24 e conclusioni. – *Riferimenti bibliografici*.

1. *Intelligenza artificiale e responsabilità penale: una premessa.*

L'art. 26 della legge 23 settembre 2025, n. 132 – rubricato «Modifiche al codice penale e ad ulteriori disposizioni penali» – introduce nel nostro ordinamento diverse norme di rilievo penalistico:

- una fattispecie di illecita diffusione di contenuti generati o manipolati artificialmente (v. *infra*, par. 3);
- una figura di reato in materia di violazione del diritto d'autore (v. *infra*, par. 4);
- una circostanza aggravante comune e alcune circostanze aggravanti speciali (v. *infra*, par. 5).

Prima di passare in rassegna le disposizioni contenute nell'art. 26, e nell'ottica di valutare queste ultime con maggiore ponderazione, può essere utile spendere qualche parola sull'impatto che l'intelligenza artificiale potrebbe avere sull'imputazione penale [1].

[1] La letteratura in argomento è ormai di ampiezza considerevole. Limitandoci alle monografie pubblicate in Italia, e senza alcuna pretesa di esaustività, v., per quanto riguarda il settore

In estrema sintesi, ci pare di poter affermare che lo sviluppo e l'utilizzo dei sistemi di IA possa sollevare due questioni di rilievo per il penalista sostanziale:

(i) per un verso, la crescente capacità di adattamento dei sistemi di IA 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 supervisionarlo [2]. 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'IA;
(ii) per altro verso, gli output dell'intelligenza artificiale possono essere utilizzati

---

delle auto a guida autonoma, M. LANZI, Self-driving cars *e responsabilità penale. La gestione del "rischio stradale" nell'era dell'intelligenza artificiale*, Giappichelli, Torino, 2023; nel settore dell'*healthcare*, 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, Bologna, 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, Torino, 2024; per un approccio trasversale ai vari settori di applicazione dell'IA. v. A. GIANNINI, *Criminal behavior and Accountability of Artificial Intelligence Systems*, Eleven, The Hague, 2023; L. D'AMICO, *La misura della (im)prevedibilità. Modelli d'imputazione della responsabilità al tempo dell'intelligenza artificiale*, ESI, Napoli, 2025; volendo, v. anche B. FRAGASSO, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla luce di una tecnologia "imprevedibile"*, Giappichelli, Torino, 2025. L'interesse della dottrina penalistica per i c.d. *AI-crimes* è altresì testimoniato dall'attenzione che l'*Association Internationale de Droit Pénal* (AIDP) ha già ampiamente riservato al tema, tanto da decidere di dedicare proprio ai rapporti tra diritto penale e intelligenza artificiale i lavori dell'ultimo Congresso internazionale, tenutosi a Parigi nel giugno 2024; a tal proposito v. la *Resolution on Traditional Criminal Law Categories And AI*, contenuta, insieme al rapporto generale (a cura di L. PICOTTI) e ad una selezione dei rapporti nazionali, in L. PICOTTI, B. PANATTONI (eds.), *Traditional Criminal Law Categories and AI: Crisi or Paligenesis? International Colloquium Section I, Siracusa, 15-16 September 2022*, in *Revue Internationale de Droit Pénal*, n. 1/2023.

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

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 n. 132/2025 parrebbe incidere – attraverso le disposizioni contenute nell'art. 26 – soprattutto sulla questione *sub* (ii), introducendo figure di reato e aggravanti volte a contrastare nuove forme di aggressione a beni giuridici realizzate *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, all'art. 24, di una delega volta ad introdurre, da un lato, delle *fattispecie di pericolo*, e, dall'altro lato, alcune *forme di limitazione della responsabilità penale*.

2. *La definizione di intelligenza artificiale come elemento normativo delle disposizioni penali (rinvio).*

Delineate, seppur curiosamente, le implicazioni che l'intelligenza artificiale potrebbe avere sulla responsabilità penale, passiamo ora all'esame delle disposizioni contenute nell'art. 26 della legge n. 132/2025.

Minimo comune denominatore di tutte le nuove norme, innanzitutto, è il riferimento al "sistema di IA" quale elemento normativo. Una riflessione sulla definizione di "sistema di IA" adottata dalla legge è dunque d'obbligo, e preliminare rispetto alla disamina delle singole disposizioni penalistiche.

L'art. 2, lett. a) della legge, in particolare, rinvia all'art. 3, par. 1, n. 1, AI Act, che definisce un "sistema di IA" 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».

Nel rinviare ai contributi di Sánchez Barrilao, Aguilar Calahorro e Burelli,

in questo volume, per l'analisi di tale definizione, ci limitiamo qui a 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 europea [3], 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 tempo [4].

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 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 IA 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 pletora di diverse proposte definitorie, spesso vaghe e sfuggenti [5]. 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

[3] Sulle modifiche subìte dalla norma definitoria nel corso del processo di approvazione del Regolamento, v. diffusamente C. TRINCADO CASTÀN, *The legal concept of artificial intelligence: the debate surrounding the definition of AI System in the AI Act*, in *BioLaw Journal-Riv. BioDiritto*, n. 1/2024, p. 305 ss.

[4] In questo senso v., per tutti, J. MÖKANDER *et al.*, *Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation*, in *Minds and Machines*, n. 32/2022, p. 245.

[5] 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.

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 IA.

Nell'immediato, invece, la questione è più complicata. Se è vero che potranno essere classificati agevolmente come sistemi di IA 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.

3. *La fattispecie di illecita diffusione di contenuti generati o manipolati artificialmente.*

La prima tra le fattispecie di reato introdotte dall'art. 26 della legge n. 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».

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 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» [6].

Stante l'indeterminatezza nella descrizione dell'evento, si deve ritenere che il

[6] V. art. 3, par. 1, n. 60, AI Act, cit.

danno ingiusto non debba necessariamente avere un contenuto patrimoniale [7]. 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» [8].

Scopo di tutela della fattispecie sembrerebbe essere costituito, innanzitutto, dalle condotte di diffusione non consensuale di *deepfakes porn*, ovverosia 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 sessuale [9].

Nel nostro ordinamento, effettivamente, mancavano 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* [10]. 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» (comma 1), ove per "immagini virtuali" si intendono le «immagini realizzate con tecniche di elaborazione grafica non associate in tutto

---

[7] In questo senso, F. CONSULICH, *Il diritto penale al tempo dell'intelligenza artificiale prospettive punitive nazionali dopo l'AI Act*, in *Dir. dif.*, n. 3-4/ 2023, p. 740; S. DE FLAMMINEIS, *Fattispecie penali nel contesto dell'intelligenza artificiale. Lo spunto del d.d.l. 1146/2024*, in *Sistema penale*, n. 9/2024, p. 9.

[8] Relazione illustrativa al d.d.l. n. S. 1146/2024, cit., p. 16.

[9] 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. PERŠAK, 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 privatezza e riservatezza*, Giappichelli, Torino, 2024, p. 157 ss.

[10] 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.

o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali» (comma 2).

Prima che venisse approvata la legge n. 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. [11]. 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 domestica [12], che richiede agli Stati membri che venga incriminata la seguente condotta intenzionale: «produrre, manipolare o alterare e successivamente rendere accessibile al pubblico, tramite TIC [13], 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» [14].

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

---

[11] 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.

[12] 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.

[13] Tecnologie dell'informazione e della comunicazione.

[14] 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».

Se la legge n. 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 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 ucraino [15].

Un indice nel senso di ritenere che queste siano le intenzioni del legislatore può essere tratto dal comma 2 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» [16].

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 democratiche [17]. Con riferimento a queste ipotesi, insomma, un reato di danno rischia di essere, come è stato osservato, "inadeguato per difetto" [18].

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

---

[15] 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. BERGSTROM, V. MITSILEGAS (eds.), *EU Law in the Digital Age*, Hart, Oxford, 2025, p. 185 ss.; T. GUERINI, Fake news *e diritto penale*, Giappichelli, Torino, 2020, p. 45 ss.

[16] 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*, in *Sistema penale*, n. 12/2024, p. 64.

[17] In argomento v., per tutti, T. GUERINI, Fake news *e diritto penale*, cit., *passim*, a cui si rinvia per un esame delle proposte di legge presentate in Italia e all'estero per contrastare il fenomeno della disinformazione.

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

dei beni giuridici offesi avrebbe reso il reato maggiormente aderente ai principi di legalità e offensività [19].

4. *La nuova fattispecie in materia di diritto d'autore.*

L'art. 26, comma 3, legge n. 132/2025 introduce una nuova fattispecie all'art. 171, comma 1, lett. a-*ter*), legge 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 artt. 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, legge n. 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, ecc.).

La nuova figura di reato mira a contrastare il fenomeno del c.d. *data scraping*, ovverosia di quella pratica di estrazione massiva, indiscriminata e non autorizzata di contenuti pubblicati *online*, finalizzata ad addestrare i modelli di IA. 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 IA generativa, ChatGPT, grazie all'utilizzo non autorizzato di articoli e libri scientifici [20] e di contributi pubblicati sui siti dei quotidiani [21].

---

[19] 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, Torino, 2024, pp. 304-305, che parla di «omnicomprensivo (quanto pericoloso) veicolo di una repressione penale illimitata e para-civilistica dei "danni" cagionati mediante l'intelligenza artificiale generativa, risultando quindi maldestra reazione simbolica a un fenomeno di crescente allarme sociale».

[20] In argomento v. E. CREAMER, *Authors file a lawsuit against OpenAI for unlawfully 'ingesting' their books*, in *The Guardian*, 5 luglio 2023.

[21] Cfr. 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.

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 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) [22].

Segnaliamo, per inciso, che la nuova fattispecie – così come, d'altronde, tutte le altre fattispecie già previste dalla legge n. 633/1941 – deve essere letta alla luce dell'art. 25 della legge n. 132/2025, che specifica che la protezione garantita dalla legge sul diritto d'autore si intende riferita alle sole opere di ingegno «umane», anche laddove «create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del lavoro intellettuale dell'autore» [23]. Ne risulta precisato, dunque, il campo di applicazione dei reati contenuti nella legge n. 633/1941, che puniscono la diffusione e la riproduzione senza diritto di opere d'ingegno (v., in particolare, gli artt. 171 ss.).

5. *Le nuove circostanze aggravanti.*

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

L'aggravante comune si va ad aggiungere, al n. 11-*undecies*, al lungo elenco di circostanze previste all'art. 61, comma 1, c.p. [24]. 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

---

[22] 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.

[23] V. art. 1, comma 1, legge 22 aprile 1941, n. 633, così come modificato dall'art. 25, comma 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).

[24] Si noti, per inciso, che in un primo momento l'aggravante era stata collocata al n. 11-*decies* dell'art. 61 c.p., che tuttavia esisteva già, con il risultato che inizialmente l'art. 61 c.p. *conteneva due n 11-decies*. L'errore materiale è stato poi corretto dall'avviso di rettifica contenuto nella *G.U.*, Serie generale n. 242 del 17 ottobre 2025.

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».

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 IA. Le fattispecie aggravate, in particolare, sono le seguenti: attentati contro i diritti politici del cittadino (art. 294 c.p.), aggiotaggio (art. 2637 c.c.), manipolazione del mercato (art. 185, d.lgs. 24 febbraio 1998, n. 58) [25].

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 IA 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 IA 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 IA, considerati *ex se* come "strumenti" insidiosi per l'aggressione ai beni giuridici tutelati dalle fattispecie incriminatrici [26]: una soluzione che non convince del tutto, dal momento che l'ampia definizione di intelligenza artificiale adottata dalla legge – sulla quale v. *supra*, par. 2 – 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 IA, 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 aggravanti [27].

---

[25] Si badi, a quest'ultimo proposito, che la legge identifica, quale pena "aggravata" per la manipolazione del mercato realizzata attraverso sistemi di IA, 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 *Sistema penale*, 17 ottobre 2025.

[26] In questo senso v. S. DE FLAMMINEIS, *Fattispecie penali nel contesto dell'intelligenza artificiale*, cit., p. 8.

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

Ecco, dunque, che se in un caso di truffa attuata con l'utilizzo di *deepfakes* l'intelligenza artificiale pare davvero come uno strumento nelle mani dell'utilizzatore, lo stesso potrebbe non accadere in relazione alle fattispecie di aggiotaggio 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'IA potrebbe fuoriuscire dalla sfera della *rappresentazione e volizione* dell'operatore umano [28].

6. *Brevi cenni ai criteri di delega in materia penale contenuti nell'art. 24 e conclusioni.*

Dalla lettura complessiva dell'art. 26 della legge n. 132/2025 si evince che il legislatore sembra concepire il sistema di IA, in ambito doloso, come mero *strumento* per la commissione di reati: le fattispecie di reato e le circostanze aggravanti introdotte dalla legge, infatti, presuppongono un nesso di diretta strumentalità tra l'agente umano e il sistema di IA, e un pieno controllo del primo rispetto al secondo.

Diversa sembra invece la consapevolezza circa i rischi dell'IA per quanto riguarda l'imputazione colposa. È da questo punto di osservazione che, a nostro avviso, deve essere letta la delega al Governo in materia penale prevista dall'art. 24 della legge n. 132/2025. Nel rinviare al contributo di Nardocci per una panoramica più ampia sul tema, ci limitiamo qui a sottolineare che dai criteri di delega relativi ai «casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale» si coglie la consapevolezza del legislatore che il "comportamento" dei sistemi di IA potrebbe sfuggire alle capacità di controllo umane.

Da un lato, infatti, al legislatore delegato si richiede la «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*

[28] 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.*, n. 3/2022, p. 1031 ss.; ID., *Il nastro di Möbius*, *Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa*, 71, 2, 2018, p. 195 ss.

tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente» (art. 24, comma 5, lett. c), enfasi aggiunta); dall'altro lato, si prevede l'introduzione di reati che anticipino la tutela penale allo stadio della *creazione del pericolo* (art. 24, comma 5, lett. b), nell'idea che l'*evento di danno* – frutto dell'imprevedibilità dell'attività algoritmica – non sempre potrà essere personalmente rimproverato all'agente umano.

La sensazione complessiva che si ha, leggendo le disposizioni di rilievo penalistico contenute nella legge n. 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 IA 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 IA;
– in secondo luogo, come garantire – attraverso una limitazione della responsabilità penale – che la persona incaricata della supervisione 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, in forza della loro afflittività, alla *matière pénale* [29] – destinato ad applicarsi ai produttori e agli utilizzatori professionali dei sistemi di IA che non rispettino le disposizioni contenute nel Regolamento.

[29] 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».

Riferimenti bibliografici.

AMORE N., *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, Bologna, 2023.

CALETTI G.M., Habeas corpus *digitale. Lo statuto penale dell'immagine corporea tra privatezza e riservatezza*, Giappichelli, Torino, 2024.

CONSULICH F., *Il nastro di Möbius*, *Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa*, 71, 2, 2018, p. 195 ss.

CONSULICH F., Flash offenders. *Le prospettive di accountability penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. proc. pen.*, n. 3/2022, p. 1015 ss.

CONSULICH F., *Il diritto penale al tempo dell'intelligenza artificiale prospettive punitive nazionali dopo l'AI Act*, in *Dir. dif.*, n. 3-4/2023, p. 721 ss.

CREAMER E., *Authors file a lawsuit against OpenAI for unlawfully 'ingesting' their books*, in *The Guardian*, 5 luglio 2023.

D'AMICO L., *La misura della (im)prevedibilità. Modelli d'imputazione della responsabilità al tempo dell'intelligenza artificiale*, ESI, Napoli, 2025.

DE FLAMMINEIS S., *Fattispecie penali nel contesto dell'intelligenza artificiale. Lo spunto del d.d.l. 1146/2024*, in *Sistema penale*, n. 9/2024.

FIORINELLI G., *La violenza mediata dalla tecnologia. Dogmatica, profili politico-criminali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digitali*, Giappichelli, Torino, 2024.

FRAGASSO B., *Intelligenza artificiale e responsabilità penale. Principi e categorie alla luce di una tecnologia "imprevedibile"*, Giappichelli, Torino, 2025.

GIANNINI A., *Criminal behavior and Accountability of Artificial Intelligence Systems*, Eleven, The Hague, 2023.

GRYNBAUM M.M., MAC R., *The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work*, in *The New York Times*, 27 dicembre 2023.

GUERINI T., Fake news *e diritto penale*, Giappichelli, Torino, 2020.

GULLO A., FLOR R., *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. 183 ss.

LANZI M., Self-driving cars *e responsabilità penale. La gestione del "rischio stradale" nell'era dell'intelligenza artificiale*, Giappichelli, Torino, 2023.

LOMBARDI O., *Responsabilità penale dell'uomo per il danno cagionato attraverso condotte dolose e colpose nell'impiego dei sistemi di intelligenza artificiale*, in *Sistema penale*, 12, 2024.

MANGIONE A., *Intelligenza artificiale, attività d'impresa e diritto penale. La «funzione di garanzia»* nell*'organizzazione e dell'organizzazione per la «sorveglianza dell'AI»*, Giappichelli, Torino, 2024.

MÖKANDER J. *et al.*, *Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation*, in *Minds and Machines*, n. 32/2022, p. 241 ss.

MUCCIARELLI F., *Intelligenza artificiale e condotte manipolative su strumenti finanziari: una nuova aggravante con effetto attenuante*, in *Sistema penale*, 17 ottobre 2025.

PICOTTI L., PANATTONI B. (eds.), *Traditional Criminal Law Categories and AI: Crisi or Paligenesis? International Colloquium Section I, Siracusa, 15-16 September 2022*, in *Revue Internationale de Droit Pénal*, n. 1/2023.

SALVI C., *Emerging trends in criminalising deepfake pornography: challenges and perspectives*, in G. VERMEULEN, N. PERŠAK, 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.

SALVI C., *The Challenges of Deepfake Technology in the Context of Political Disinformation*, in M. BERGSTROM, V. MITSILEGAS (eds.), *EU Law in the Digital Age*, Hart, Oxford, 2025, p. 185 ss.

TRINCADO CASTÀN C., *The legal concept of artificial intelligence: the debate surrounding the definition of AI System in the AI Act*, in *BioLaw Journal-Riv. BioDiritto*, n. 1/2024, p. 305 ss.