

## I CONTENUTI PENALI DELLA LEGGE SULL'INTELLIGENZA ARTIFICIALE \*

di Lorenzo Picotti

*Il saggio analizza i contenuti penali della recente legge sull'intelligenza artificiale del 23.9.2025, n.132, muovendo dalla sua collocazione nell'articolato contesto extra penale, rappresentato soprattutto dal regolamento sull'intelligenza artificiale dell'Unione europea 2024/1689 (c.d. AI Act), cui la legge fa espresso rinvio in alcune disposizioni, contenendo altresì deleghe per l'adeguamento della normativa interna. In particolare sono analizzati i due nuovi delitti, ormai in vigore, di illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale (art. 612-quater c.p.:\_c.d. deep fake), rispetto a cui viene evidenziato quale sia il nuovo bene giuridico protetto, e di violazione del diritto d'autore nell'estrazione di dati per i sistemi di intelligenza artificiale (nuova lettera a – ter aggiunta all'art. 171, comma 1, legge 633/1941). Quindi sono esaminate la circostanza aggravante comune, aggiunta con il numero 11-undecies all'art. 61 c.p., e quelle speciali introdotte nel codice a rafforzamento della tutela dei diritti politici dei cittadini, e nella legislazione speciale, in materia di manipolazioni del mercato. Infine, vengono esposti i contenuti delle norme di delegazione in materia penale, che porteranno – senza chiari criteri direttivi - all'introduzione di nuovi reati, dolosi o colposi, per l'omessa adozione di misure di sicurezza, oltre che ad una "precisazione" dei criteri di imputazione della responsabilità penale delle persone fisiche e di quella amministrativa degli enti per illeciti inerenti a sistemi di intelligenza artificiale. Nelle osservazioni conclusive, pur riconoscendosi che la legge rappresenta un passo importante per la sua dimensione strutturale che investe svariati settori, si criticano le incongruenze rilevate e soprattutto la prospettiva "panpenalistica" che punta sulla creazione di nuovi reati e sull'aggravamento delle pene, mentre il diritto penale dovrebbe rappresentare l'ultima ratio di tutela e governo della materia.*

SOMMARIO: 1. Introduzione: il contesto extra penale. – 2. La collocazione ed articolazione delle disposizioni che riguardano esplicitamente la materia penale. – 3. Le nuove fattispecie incriminatrici in vigore. – 3.1. L'illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale (art. 612-quater c.p.). – 3.2. La nuova ipotesi di violazione del diritto cd'autore nell'estrazione di dati per i sistemi di intelligenza artificiale. – 4. Le circostanze aggravanti. – 4.1. La nuova circostanza aggravante comune (art. 61 n. 11-undecies c.p.). – 4.2. Le circostanze aggravanti speciali introdotte nel codice e nella legislazione speciale. – 5. Sulle norme di delegazione in materia penale. – 6. Osservazioni conclusive.

---

\* Il presente contributo è una limitata rielaborazione dell'omonimo Capitolo destinato al volume *“La disciplina italiana sull'intelligenza artificiale”* a cura di Giuseppe Cassano ed Enzo Maria Tropodi, in corso di stampa per l'editore Pacini.

## 1. Introduzione: il contesto extra penale.

Il commento delle norme penali contenute nella recente legge sull'intelligenza artificiale<sup>1</sup> richiede, preliminarmente, un seppur veloce inquadramento nel contesto più ampio in cui si colloca.

Infatti, come si legge già nell'art. 1, che riguarda le finalità e l'ambito di applicazione, la normativa nazionale deve adeguare l'ordinamento interno al quadro definito dal regolamento generale sull'intelligenza artificiale dell'Unione europea 2024/1689 (d'ora in poi *AI Act*), al quale quindi, per il principio di primazia del diritto europeo, sia la legislazione, come prevede genericamente, quale primo oggetto delle deleghe legislative, l'art. 24, comma 1, che l'interpretazione e l'applicazione delle norme interne devono conformarsi, come ricorda, se ve ne fosse bisogno, il secondo comma della prima disposizione citata.

Essendo il regolamento del Parlamento europeo e del Consiglio una fonte di applicazione diretta negli Stati membri, che garantisce l'uniformità della disciplina in tutta l'Unione e pertanto non solo non richiede, ma anzi esclude che se ne dia tecnicamente un'attuazione con disposizioni interne che potrebbero divergere fra gli Stati membri (come accade invece per le direttive, che lasciano loro margini di autonomia, specie in materia penale), le "definizioni" contenute nell'art. 2 della legge, concernenti, in particolare, la fondamentale nozione extra-penale di "*sistema di intelligenza artificiale*" (lettera a), elemento cardine, c.d. normativo, anche della gran parte delle disposizioni penali che si esamineranno, nonché quella di "*modelli di intelligenza artificiale*" (lettera c), che parimenti viene in rilievo in talune ipotesi, non vengono fornite dalla legge nazionale, che opera un rinvio espresso, c.d. recettizio, alle corrispondenti definizioni già contenute nell'*AI Act*<sup>2</sup>.

Oltre a dover rispettare tali principi e definizioni, la disciplina penale deve anche conformarsi ad alcune specifiche «*Disposizioni di settore*», cui è dedicato il Capo II della legge, che possono integrare anche diversi elementi di fattispecie incriminatrici ed avere, quindi, rilievo indiretto per fondare o delimitare altresì la responsabilità penale. Ad esempio, per quel che riguarda l'ambito sanitario e la ricerca e sperimentazione scientifica (artt. da 7 a 10), come già ho avuto modo di evidenziare in precedenti

---

<sup>1</sup> Legge 23 settembre 2025, n. 132, in G.U. n. 233 del 25.9.2025, in vigore dal 10.10.2025. Nel testo ogni articolo richiamato si riferisce a tale fonte, se non diversamente specificato.

<sup>2</sup> Si vedano rispettivamente l'art. 3, punto 1, e l'art. 3, punto 63, *AI Act*, su cui si tornerà. Solo la definizione assai ampia di «*dato*» è invece fornita dalla lettera b) del citato art. 1, che in realtà riproduce alla lettera (salvo usare il singolare) quella già contenuta nell'art. 2, numero 1) del Regolamento (Ue) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati), che così recita: «1) «*dati*»: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva». Per la sua ampiezza, tale definizione si distingue invece da quella di «*dato personale*», che compariva nel Codice privacy (d.lgs. 30.6.2023, n. 196 e s.m.i.), ed è ora sostituita da quella di cui all'art. 4, n. 1 del regolamento (UE) 2016/679 (GDPR), che così recita: «*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")*».

contributi<sup>3</sup>, talune disposizioni interessano reati di cui la legge in esame non si occupa espressamente, quali gli omicidi colposi o le lesioni personali colpose, ovvero le violazioni delle disposizioni in materia di trattamento dei dati personali, che possono emergere nelle attività in ambito sanitario o nella ricerca e sperimentazione scientifica.

## **2. La collocazione ed articolazione delle disposizioni che riguardano esplicitamente la materia penale.**

Venendo a considerare le disposizioni della legge che riguardano *esplicitamente* la materia penale, appare opportuno evidenziare, in via preliminare, quale sia la loro (disomogenea) collocazione sistematica.

Va innanzitutto menzionato il Capo V intitolato espressamente «*Disposizioni penali*», costituito per vero dal solo art. 26, che introduce due nuovi delitti.

Alla lettera c) del comma 1 aggiunge al codice penale l'art. 612-*quater*, che punisce l'«*Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*» (di cui si dirà *infra*, par. 3.1), mentre al comma 3 aggiunge una nuova fattispecie delittuosa (la lettera a-*ter*) all'art. 171, primo comma, della legge 22 aprile 1942, n. 633 s.m.i. sul diritto d'autore (di cui si dirà *infra*, par. 3.2).

Lo stesso art. 26 della legge aggiunge poi quattro nuove circostanze aggravanti.

Con il comma 1, lettera a), prevede quella comune di cui al numero 11-*undecies* dell'art. 61 c.p. (di cui si dirà *infra*, par. 4.1), mentre alla lettera b) dello stesso comma prevede una circostanza aggravante speciale per il delitto di «*Attentati contro i diritti politici dei cittadini*» di cui all'art. 294 c.p., di cui si dirà *infra*, par. 4.2.1.

Altre due circostanze aggravanti speciali sono infine inserite dai commi 2 e 4 in altrettante fattispecie delittuose previste da leggi extra codice, ed in particolare in materia di aggio, sia c.d. societario (*ex* art. 2637 c.c.), sia c.d. finanziario (manipolazione del mercato *ex* art. 185, comma 1, d.lgs. 24 febbraio 1998, n. 58 s.m.i., recante il Testo unico delle disposizioni in materia di intermediazione finanziaria, d'ora in poi TUF), di cui si dirà *infra*, par. 4.2.2.

Il quadro delle disposizioni che toccano la materia penale non si esaurisce però qui.

Infatti, il diritto penale è interessato anche da ulteriori disposizioni, collocate sia nel Capo IV, che riguarda la «*Tutela del diritto d'autore delle opere generate con l'ausilio dell'intelligenza artificiale*», costituito anch'esso da un solo articolo, l'art. 25, che integra la citata legge 633/1941 sul diritto d'autore (di cui si dirà *infra*, par. 3.2), sia nel Capo III contenente invece «*Deleghe legislative al Governo*» (art. 24) per l'emanazione – entro 12 mesi dall'entrata in vigore della legge – di un complesso assai ampio ed articolato di disposizioni aventi valore di legge, che in una parte assai rilevante riguardano anche la materia penale (si veda *infra* par. 5).

---

<sup>3</sup> Sia consentito rinviare a L. PICOTTI, *Sanità digitale ed intelligenza artificiale: profili penali*, in *Dir. Internet*, 2024, p. 415 s., ed ai richiami bibliografici e normativi ivi contenuti.

### 3. Le nuove fattispecie incriminatrici in vigore.

3.1. *L'illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale (art. 612-quater c.p.).*

Muovendo dall'analisi delle due nuove fattispecie penali introdotte dalla legge, che sono in vigore dal 10 ottobre 2025, un ruolo preminente ha il delitto di cui all'articolo 612-quater c.p., introdotto nel Titolo XII del codice penale, dedicato ai "delitti contro la persona" ed, in particolare, nella Sezione III intitolata ai "delitti contro la libertà morale" dell'esteso Capo III, in cui sono raccolti tutti i delitti "contro la libertà individuale".

La collocazione è significativa, per definire quale sia il bene giuridico protetto, dato che esprime un'esigenza nuova di protezione della "persona", espressamente indicata come vittima dal testo normativo, esposta ai pericoli creati dalle più moderne tecnologie informatiche e delle comunicazioni (c.d. TIC – in inglese ICT)<sup>4</sup>, che oggi consentono anche di produrre «mediante l'impiego di sistemi di intelligenza artificiale» contenuti non genuini, quali «immagini, video o voci» che non provengono o non esprimono quanto sembrerebbe attribuibile al soggetto od alla realtà che appare.

Si tratta del riconoscimento di un diritto nuovo, che va oltre i beni tradizionali dell'onore, della reputazione o della riservatezza, cui si sono invece riferiti i primi commenti<sup>5</sup>, e che si può sintetizzare in quello di non essere ingannati o condizionati sfavorevolmente dall'intelligenza artificiale. Si tratta di un interesse primario, nella prospettiva di una sua regolamentazione basta sulla primazia dell'uomo, certamente meritevole di tutela, anche penale, che trova già un chiaro fondamento normativo nell'art. 5 lettera a) *AI Act*. Tale disposizione vieta infatti in modo assoluto sia «le tecniche subliminali che agiscono senza che una persona ne sia consapevole» sia le «**tecniche volutamente manipolative o ingannevoli** aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona» [...] «pregiudicando in modo considerevole la [...] capacità di prendere una decisione informata [...] **in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo**»<sup>6</sup>, considerate pratiche in sé illecite, che comportano rischi

---

<sup>4</sup> Per un quadro di tale tematica anteriore all'avvento dell'intelligenza artificiale, si possono vedere i molteplici contributi raccolti nel volume da me curato *Tutela penale della persona e nuove tecnologie. Quaderni per la riforma del codice penale*, Padova, 2013.

<sup>5</sup> B. FRAGASSO, [Profili penalistici della legge sull'intelligenza artificiale: osservazioni a prima lettura](#), in questa Rivista, 16 ottobre 2025, in specie par. 5.1, che parla di offesa alla reputazione, all'intimità, alla riservatezza ed anche autodeterminazione nella sfera sessuale.

<sup>6</sup> Riporto per completezza, oltre al testo integrale della lettera a), anche quello della lettera b) dell'art. 5 *AI Act*, che riguarda specificamente le "persone vulnerabili": «a) *l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso,*

inaccettabili, e per questo già oggi punibili con le più severe delle sanzioni amministrative stabilite dall'art. 99, al par. 3, *AI Act* <sup>7</sup>.

È un diritto che fa capo a qualunque “*persona*” cessionaria di tali prodotti, ovvero destinataria della loro comunicazione o diffusione, anche attraverso le ampie possibilità di accesso che le nuove tecnologie consentono<sup>8</sup>. Diritto peraltro disponibile, restando la persona libera di consentire o meno, come emerge dall'elemento, espresso negativamente, della *manca di consenso*, costitutivo della fattispecie<sup>9</sup>. L'offesa di tale nuovo bene giuridico è però considerata dal legislatore meritevole di tutela penale solo nei limiti in cui produca anche un “*danno ingiusto*”, che rappresenta l'evento consumativo, peraltro di ampia portata, che deve dunque essere oggetto anche del dolo dell'agente, su cui si tornerà dopo aver analizzato le condotte che debbono cagionarlo.

La collocazione subito dopo l'art. 612-ter c.p., introdotto nel 2019, che punisce la “*diffusione illecita di immagini o video sessualmente espliciti*” (delitto impropriamente definito *revenge porn*)<sup>10</sup>, evidenzia l'espansione del novero dei rischi per i diritti della persona nell'attuale società tecnologica, in quanto – pur rinvenendosi alcuni elementi comuni – il bene giuridico protetto da questa precedente norma è ben più limitato e riconducibile, questo sì, alla ristretta sfera della riservatezza ed autodeterminazione della persona, nel campo della sessualità, di fronte a condotte, peraltro, analoghe di

*in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo;*

*b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo».*

<sup>7</sup> Che così recita: «3. La non conformità al divieto delle pratiche di IA di cui all'articolo 5 è soggetta a 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». Sulla opportunità di presidiare anche con sanzioni penali a livello nazionale la violazione del divieto delle pratiche illecite elencate, nel citato art. 5 *AI Act*, mi ero già espresso nel contributo [Categorie tradizionali del diritto penale e intelligenza artificiale: crisi o palinogenesi?](#) in questa Rivista, 31 luglio 2024, par. 3.3.2.1, p. 11.

<sup>8</sup> Che l'accesso «mediante la rete» si ponga ormai quale alternativa sostanzialmente equivalente, seppur ritenuta meno grave dal nostro legislatore, rispetto alle condotte di “*detenzione*”, di cui all'art. 600-*quater* c.p., oltre che di “*diffusione*”, “*pubblicizzazione*” e “*comunicazione*” di cui ai commi 3 e 4 dell'art. 600-*ter* c.p., aventi ad oggetto materiale pedopornografico, emerge normativamente dal suo espresso inserimento nell'ultimo comma della prima disposizione citata, da parte dell'art. 20, comma 1, lett. a), n. 1), legge 23 dicembre 2021, n. 238 (c.d. legge europea), con cui è stata chiusa la procedura di infrazione promossa dalla Commissione europea proprio perché fosse così data piena attuazione alla direttiva [2011/93/UE](#) in materia.

<sup>9</sup> Sulla distinzione dogmatica, che ha rilevanti conseguenze anche pratiche, in particolare sull'oggetto del dolo, fra le ipotesi in cui la mancanza di consenso è elemento costitutivo della fattispecie (espresso negativamente) e le ipotesi in cui invece il consenso dell'avente diritto integra la causa di giustificazione di cui all'art. 50 c.p., basti qui il rinvio, nell'ampia letteratura e manualistica, a M. ROMANO, *Commentario sistematico del Codice penale*, 3<sup>a</sup> ed., Milano 2004, sub Art. 50, § I, n. 4, p. 528 s.; F. VIGANÒ, *Art. 50*, n. 8, in E. DOLCINI, G.L. GATTA (cur.), *Codice penale commentato*, I, 5<sup>a</sup> ed., Milano 2021, § II, n. 8, p. 825 s.

<sup>10</sup> Per la precisione, dall'art. 10, comma 1, [legge 19 luglio 2019, n. 69](#), cui sono succedute modifiche sul regime di procedibilità e sull'entità delle pene. In materia si veda l'ampia indagine di G.M. CALETTI, *Habeas corpus digitale. Lo statuto penale dell'immagine corporea tra riservatezza e riservatezza*, Torino, 2024, in specie p. 217 s.

cessione, pubblicazione o diffusione, facilitate enormemente dalle nuove tecnologie, ferma in entrambe le fattispecie la condizione della mancanza di consenso.

Nel nuovo reato in commento, come detto, viene tutelato invece *qualunque contenuto* di «video» o «immagini», cui si aggiungono anche le «voci», da ogni «falsificazione» o «alterazione» realizzata «mediante sistemi di intelligenza artificiale» che sia idonea ad «indurre in inganno sulla loro genuinità». Elementi tutti estranei alla precedente fattispecie, che incidono dunque sull'identificazione del nuovo bene giuridico tutelato nei termini sopra precisati, non essendo riducibile né alla generica «reputazione» né all'«autodeterminazione» tantomeno nella sola sfera sessuale, anche se è il c.d. *porn deep fake* che appare criminologicamente il più diffuso e maggiormente oggetto (al momento) d'attenzione mediatica<sup>11</sup>.

Il fatto tipico presenta, dunque, molteplici e differenti requisiti oggettivi, fra cui spicca, per la sua novità, quello del *mezzo* che deve tassativamente essere rappresentato da un «sistema di intelligenza artificiale», la cui definizione, come si è premesso, va ricavata dall'art. 3, punto 1 dell'*AI Act*<sup>12</sup> cui l'art. 2, lettera a) della legge fa espresso rinvio.

Si tratta di una nozione extrapenale assai ampia, oggetto anche di critiche sul piano giuridico e scientifico, soprattutto per l'inevitabile molteplicità, complessità e mutevolezza delle diverse tecniche applicabili, in continua evoluzione, rispetto a quelle richiamate.

Tuttavia, ritengo che essa debba accettarsi, non solo sul piano strettamente giuridico per la primazia del diritto dell'Unione, ma anche perché coglie le essenziali caratteristiche distintive rispetto alla nozione tradizionale di «sistema informatico» (o «computer system»), quale definita dall'art. 1, lettera a) della Convenzione *Cybercrime* del Consiglio d'Europa (CETS No. 185) aperta alla firma a Budapest il 23 novembre 2001, imperniata ancora sulla struttura materiale di un «apparecchio» («device») od anche di un gruppo di più apparecchi, interconnessi o correlati, uno o più dei quali «in esecuzione di un programma» realizzi «un'elaborazione automatica di dati»<sup>13</sup>.

Un sistema di intelligenza artificiale, viceversa, pur potendo essere ricondotto – a certe condizioni – a tale categoria generale, si connota *esclusivamente* sul piano *funzionale*, per la sua «autonomia» ed «adattabilità», che ne qualifica la specifica «capacità di generare» un *out put* in conformità a determinati «obiettivi», ed abbia così la potenzialità

<sup>11</sup> Cfr. per tutti G.M. CALETTI, *Habeas corpus digitale*, cit., p. 160 s.

<sup>12</sup> Così definito dall'art. 3, punto 1 *AI Act*: «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».

<sup>13</sup> Nel testo ufficiale inglese: «'computer system' means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data». Tale definizione non è stata però recepita a livello legislativo nel nostro ordinamento, in cui l'elaborazione del concetto, pur integrante un elemento normativo di molte fattispecie penali, resta affidata all'elaborazione giurisprudenziale (e dottrinale). Per un generale bilancio in parte critico sull'attuazione della Convenzione in esame e del suo Primo protocollo addizionale, sia consentito rinviare a L. PICOTTI, *I primi vent'anni della Convenzione di Budapest nell'ottica sostanzialista e la mancata ratifica ed esecuzione del Primo Protocollo addizionale contro il razzismo e la xenofobia*, in *Dir. pen. proc.*, 8/2022, p. 1028 s.

di «*influenzare ambienti fisici o virtuali*», consistendo il suo contenuto in «*previsioni, raccomandazioni o decisioni*», che anche terminologicamente alludono ad attività intellettuali, di natura cognitiva od anche volitiva, proprie dell'uomo<sup>14</sup>.

Senza certo avvalorare la tesi che si tratti di un'effettiva "intelligenza" assimilabile a quella umana, cui solo metaforicamente si può accostare<sup>15</sup>, è evidente che la *generazione* di contenuti si correla alla capacità non solo di comunicarli, ma anche di *crearli* e, per questo, di *influenzare* in modo innovativo l'ambiente esterno.

Pertanto, si tratta di requisiti distintivi, che per il loro espresso rilievo giuridico possono e debbono essere accertati in sede giudiziaria penale, al di là delle singole specifiche tipologie e tecniche informatiche che vengano utilizzate e sviluppate per assolvere alle descritte *funzioni*.

Quanto agli altri elementi della fattispecie, come appena osservato molti compaiono già in disposizioni vigenti, a partire dal menzionato art. 612-ter c.p., fino ai delitti in materia di pornografia minorile, di cui in particolare all'art. 600-ter, comma 3, c.p., che punisce le condotte consistenti nel «*pubblicizzare*» o «*diffondere*», ed all'art. 600-*quater* c.p., che punisce quella di «*cedere*» materiale informatico «*anche per via telematica*», o di consentire di avervi «*accesso mediante la rete*», la cui rilevanza dipende dalla sempre più rilevante estensione di comportamenti e rapporti che si svolgono nel *cyberspace*<sup>16</sup>.

Ma l'attenzione va richiamata anche sulle ulteriori nozioni di "*alterazione*" e "*falsificazione*" che caratterizzano l'illecito in esame, che già tradizionalmente compaiono nelle molteplici ipotesi dei delitti di falso, in specie documentale.

Solo con cautela si può fare riferimento concettuale, *mutatis mutandis*, all'elaborazione dogmatica sviluppata in proposito, dovendosene distinguere l'oggetto e lo scopo della tutela.

L'"*alterazione*" può essere intesa quale modificazione non autorizzata di un contenuto genuino, rispetto a quello creato o proveniente dal suo autore, almeno apparente; mentre la "*falsificazione*" – che include tradizionalmente il concetto più radicale di "*contraffazione*" – è da intendere quale creazione, non solo parziale, ma anche integrale, di un contenuto difforme dall'originale od, anche, dal vero obiettivo, o realtà c.d. esterna, potendo quindi consistere in un contenuto *generato* da un sistema di intelligenza artificiale del tutto indipendentemente da essa.

È, in particolare, da respingere una lettura restrittiva della condotta di "*falsificazione*" che la faccia dipendere dalla preesistenza di un contenuto genuino, che

---

<sup>14</sup> In argomento, nella ormai vasta letteratura penalistica, si veda B. FRAGASSO, *Intelligenza artificiale e responsabilità penale. Principi e categorie alla prova di una tecnologia "imprevedibile"*, Torino, 2025, in specie Parte I, cap. I, p. 17 s.; sul punto, per ragioni di sintesi, sia consentito rinviare anche al mio contributo [Ente](#), in *Scritti in onore di Carlo Enrico Paliero*, vol. III, Milano, 2023, nonché in *questa Rivista*, 10 luglio 2023.

<sup>15</sup> In argomento rinvio ai fondamentali contributi di Luciano Floridi, da ultimo (in lingua italiana), *La differenza fondamentale. Artificial Agency: una nuova filosofia dell'intelligenza artificiale*, Milano 2025.

<sup>16</sup> Per riferimenti sul crescente rilievo di tali "fatti" e sulla necessità di interpretarli alla stregua dei sottostanti "rapporti" conflittuali, pur in parte smaterializzati, sia consentito il rinvio a L. PICOTTI, *Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (cur.), *Cybercrime*, 2<sup>a</sup> ed., Milano, 2023, p. 31 s. anche per le essenziali indicazioni bibliografiche.

ne dovrebbe essere alla base, in quanto si sovrapporrebbe così alla condotta di “alterazione” e la doppia previsione sarebbe superflua.

Viceversa, nel concetto di “falsificazione” rientra l’ipotesi di creazione di un contenuto *ab origine* nuovo, materialmente ovvero anche solo ideologicamente “falso”, in quanto del tutto diverso non solo da uno genuino, ma anche dalla verità oggettiva, che solo apparentemente sembrerebbe rappresentare.

È stato già opportunamente sottolineato, che la nuova fattispecie delittuosa si estende a colpire fenomeni che vanno oltre l’offesa della sfera della riservatezza sessuale<sup>17</sup>, ravvisabile nelle manipolazioni di immagini di corpi di persone impegnate in attività sessuali, utilizzando altre immagini o creando immagini del tutto false dei volti, che facciano attribuire una falsa identità a tali corpi, spesso riferendoli a personaggi celebri, od anche a vicini/e di casa o lavoro, od a compagni/e di scuola, ecc. (c.d. *porn deep fake*).

Simili alterazioni o falsificazioni mediante sistemi di intelligenza artificiale possono, infatti, riguardare anche personaggi politici, ad esempio per far attribuire loro false dichiarazioni o prese di posizione, che possano influenzare l’opinione pubblica, gettando discredito su avversari o distorcendo la competizione politica od elettorale<sup>18</sup>.

Il fondamentale requisito selettivo che accomuna le diverse ipotesi è che tali manipolazioni siano «*idonee a indurre in inganno*» sulla loro genuinità. Oggettiva “*idoneità*” ingannatoria che va riferita dunque alle immagini, ai video o alle voci *risultanti* dalla falsificazione od alterazione, cioè all’*out put* prodotto da qualsiasi sistema di intelligenza artificiale venga impiegato, non direttamente alla sua capacità tecnica come tale, dovendosi assumere a parametro di valutazione la comune capacità di discernimento dei *destinatari* della comunicazione oggettivamente intesa<sup>19</sup>.

È già stato oggetto di critica, infine, l’ulteriore elemento oggettivo costituito dalla causazione di un “*danno ingiusto*” che rappresenta l’evento del reato, segnandone il momento consumativo. Pertanto deve non solo essere *causato* dalla condotta dell’agente, mediata però dal sistema di intelligenza artificiale, con conseguente necessità di dimostrare il relativo nesso eziologico<sup>20</sup>, ma anche essere da lui consapevolmente *voluto*, rientrando nell’oggetto del dolo.

---

<sup>17</sup> B. FRAGASSO, *Profili penalistici*, cit., par. 5.1

<sup>18</sup> Per taluni esempi di casi verificatisi si veda ancora B. FRAGASSO, *Profili penalistici*, cit., par. 5.2.

<sup>19</sup> Un riferimento interpretativo può essere ricavato dalla definizione di pedopornografia “virtuale” di cui all’art. 600-*quater*.1 c.p., che richiede che le immagini siano realizzate «*utilizzando immagini di minori degli anni diciotto o parti di esse*» mediante «*tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali*» ma la cui «*qualità di rappresentazione fa apparire come vere situazioni non reali*». In argomento cfr. G. M. CALETTI, *Habeas corpus digitale*, cit., in specie 157 s. con ulteriori indicazioni, nonché, volendo, anche per considerazioni di politica criminale, già L. PICOTTI, *I delitti di sfruttamento sessuale dei bambini, la pornografia virtuale e l’offesa dei beni giuridici*, in *Scritti per Federico Stella*, Napoli, 2007, p. 1267 s.

<sup>20</sup> Sulle difficoltà che potrebbe presentare l’accertamento del nesso eziologico fra la condotta “a monte” dell’uomo e l’evento che, nell’ultimo anello, viene prodotto mediante l’intervento del sistema di intelligenza artificiale, cfr. A. GIANNINI, *Criminal Behavior and Accountability of Artificial Intelligence Systems*, Maastricht 2023, in specie p.170 s.; sinteticamente cfr. anche L. PICOTTI, *Categorie tradizionali del diritto penale e intelligenza artificiale*, cit., par. 3.3.1, p. 9.

Tale delimitazione dell'operatività della fattispecie incriminatrice appare distonica rispetto a quanto previsto dalle altre fattispecie sopra menzionate, che si consumano con le condotte di diffusione, pubblicazione, cessione od anche mero accesso, e crea specifici problemi di accertamento dato l'apporto "autonomo" e talora "imprevedibile" del sistema di intelligenza artificiale, il cui intervento è tipizzato come necessario mezzo di realizzazione del reato<sup>21</sup>.

Diverge altresì dal "modello" dell'illecito amministrativo delineato dall'art. 5 in combinazione con l'art. 99 *AI Act*, di cui sopra si è detto (cfr. in specie note 5 e 6), per la cui consumazione è sufficiente un pericolo concreto, dovendo la condotta avere anche soltanto lo scopo, non necessariamente l'effetto, «di *distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo*» (evidenziazioni aggiunte).

Salvo, dunque, ritenere il "danno" *in re ipsa* per le caratteristiche di siffatte condotte che si realizzano nel *cyberspace*, conformato dalle tecnologie della comunicazione e dell'informazione che consentono l'immediata e globale diffusione dei dati in rete, in tempo reale, anche a chiunque acceda ai contenuti immessi, non può che suggerirsi un'interpretazione assi lata, certamente non ristretta ad un concreto danno di contenuto patrimoniale, bastando – oltre che occorrendo – che sia "ingiusto".

Requisito che deve aggiungersi all'illiceità oggettiva dell'alterazione o falsificazione, nonché a quella della diffusione senza consenso, dovendo emergere la contrarietà a o, meglio, la violazione di qualsiasi norma giuridica, che privi l'evento *in sé* di ogni giustificazione oggettiva – come si verifica in altre ipotesi di c.d. doppia ingiustizia, in cui compare una simile locuzione accanto ad una condotta già illecita<sup>22</sup>.

Una problematica ulteriore emerge se si considera il regime della procedibilità, che è a querela per l'ipotesi base, in cui il soggetto legittimato è certamente la persona che abbia subito il "danno ingiusto", fors'anche perché sarebbe difficile pretendere di individuare la vittima basandosi solo su quella che si possa ricavare da un'immagine o

---

<sup>21</sup> Sui presupposti e i limiti di imputazione della responsabilità penale alle persone umane (fisiche e giuridiche) che "stanno dietro" tali sistemi, si vedano le Raccomandazioni contenute nella *Resolution on Traditional Criminal Law Categories and AI*, approvata all'esito del Colloquio internazionale svoltosi a Siracusa il 16-17.9.2022, a conclusione dei lavori preparatori della Prima Sezione del XXI Congresso internazionale dell'*Association International de Droit Pénal* (AIDP), dedicato al tema generale "*Artificial Intelligence and Criminal Law*", svoltosi a Parigi il 25-28.6.2024. Al riguardo si rinvia al volume monografico, a cura di L. PICOTTI, B. PANATTONI, della *Revue Internationale de Droit Pénal* (RIDP), 1/2023, che oltre alla Risoluzione finale contiene anche il *Rapport général* a cura del sottoscritto e ad una selezione dei rapporti nazionali. Su questo complesso ambito problematico potrebbero (e dovrebbero) soccorrere i "criteri di imputazione della responsabilità" che le norme delegate, ai sensi dell'art. 24, comma 5, lett. c), dovrebbero "precisare" nell'ambito penale (sul punto cfr. però criticamente *infra* par. 5).

<sup>22</sup> Dalla vasta elaborazione dottrinale e giurisprudenziale sviluppata a proposito del requisito del "danno ingiusto" che compariva (al di là della sua ulteriore qualificazione in termini di "patrimonialità") nell'abrogato art. 323 c.p., è emersa la necessità di distinguere fra *ingiustizia del mezzo* ed *ingiustizia del risultato*, non potendo la seconda coincidere od essere assorbita dalla prima ("doppia ingiustizia" da riconoscere anche in altri reati contro la pubblica amministrazione, in particolare di corruzione).

voce per definizione manipolata, con la conseguenza che non potrebbe essere precisamente riconoscibile.

Tuttavia, è prevista la procedibilità d'ufficio, oltre che nel caso di connessione con un altro delitto per il quale si proceda d'ufficio (al riguardo si può pensare a fattispecie associative o ad ipotesi di estorsione *on-line*<sup>23</sup> o di *stalking* aggravato<sup>24</sup>), anche nel caso di persone incapaci per età o per un'incapacità assoluta, ed infine se sia offesa una «*pubblica autorità a causa delle funzioni esercitate*».

Tale ultima previsione porta in realtà ad estendere la stessa nozione di “*persona*” offesa da questo reato oltre l'ambito delle persone fisiche, per coinvolgere enti pubblici ed articolazioni della pubblica amministrazione, con l'incertezza se in tali casi sia comunque necessario individuare *anche* una o più persone fisiche, nell'ambito dell'ente o della pubblica amministrazione, che abbiano subito il “*danno ingiusto*” (ad es. soggetti politici nei confronti dei quali l'utilizzo del *deep fake* abbia avuto lo scopo di fomentare una propaganda di disinformazione, fino ad incidere sul corretto svolgimento di una competizione elettorale), o se invece il “*danno ingiusto*” debba o possa far capo soltanto alla stesso ente od amministrazione, andando però così il delitto oltre l'ambito di quelli “*contro la persona*”.

Va, infine, segnalato che, per attuare la recente direttiva dell'Unione europea 2024/1385 del 14 maggio 2024 sulla lotta alla violenza contro le donne e la violenza domestica, dovrà essere espressamente incriminato anche il fatto “*intenzionale*” previsto dal suo art. 5, lettera b), consistente nel «*produrre, manipolare o alterare e successivamente rendere accessibile al pubblico, tramite TIC, 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*».

Anche in tale direttiva è dunque richiesto soltanto un pericolo concreto, non un danno effettivo<sup>25</sup>: con la conseguenza che la più restrittiva previsione ricavabile dalla fattispecie nazionale in esame potrebbe essere ritenuta non conforme alle esigenze di compiuta attuazione della direttiva predetta, rendendo necessario un intervento correttivo da parte del legislatore.

### 3.2. La nuova ipotesi di violazione del diritto cd'autore nell'estrazione di dati per i sistemi di intelligenza artificiale.

Il secondo nuovo delitto che viene introdotto dalla legge in esame riguarda la specifica materia della tutela penale del diritto d'autore.

---

<sup>23</sup> Ipotesi oggi specificamente punita, quale aggravante, dal terzo comma dell'art. 629 c.p., aggiunto dall'art. 16, comma 1, lett. m), n. 2), legge 28 giugno 2024, n. 90, su cui cfr. C. CRESCIOLI, *Cybercrime e tutela penale del patrimonio. Un'indagine in prospettiva comparata*, Milano 2024, in specie p. 155 s.

<sup>24</sup> Art. 612-bis, comma 2, c.p., come così sostituito dall'art. 1, comma 3, lett. a), decreto legge 14 agosto 2013, n. 93 convertito, con modificazioni, dalla legge 15 ottobre 2013, n. 119.

<sup>25</sup> Cfr. sul punto anche B. FRAGASSO, *Profili penalistici*, cit., par. 5.1.

Infatti, l'art. 26, comma 3, aggiunge all'art. 171, primo comma, della legge 633/1941, dopo la lettera a-bis), una nuova fattispecie delittuosa, identificata con la lettera a-ter), che punisce chi «*riproduce o estrae testo o dati da opere o altri materiali disponibili in rete o in banche dati in violazione degli articoli 70-ter e 74-quater anche attraverso sistemi di intelligenza artificiale*».

La pena è peraltro risibile, se si guarda agli interessi in gioco, consistendo nella sola multa da euro 51 a euro 2.065.

Si tratta di una fattispecie c.d. meramente sanzionatoria dei precetti extra-penali cui espressamente rinvia, ed in specie di quelli stabiliti dagli articoli introdotti dal d.lgs. 8 novembre 2021, n. 177, di attuazione della direttiva (UE) 2019/790, che avevano stabilito regole per disciplinare, ma nel contempo così anche consentire alle condizioni indicate, l'attività di “*estrazione di testo e di dati*” (c.d. *text data mining*: TDM) definita – ai sensi del comma 2 dell'art. 70-ter legge 633/1941 – come «*qualsiasi tecnica automatizzata volta ad analizzare grandi quantità di testi, suoni, immagini, dati o metadati in formato digitale con lo scopo di generare informazioni, inclusi modelli, tendenze e correlazioni*».

La disciplina è ora meglio modellata dal nuovo art. 70-septies legge 633/1941, introdotto dall'art. 25 (rubricato: “*Tutela del diritto d'autore delle opere generate con l'ausilio dell'intelligenza artificiale*”) che occupa l'intero Capo IV della legge in esame, in forza del quale «*le riproduzioni e le estrazioni da opere o da altri materiali contenuti in rete o in banche dati a cui si ha legittimamente accesso, ai fini dell'estrazione di testo e di dati attraverso modelli e sistemi di intelligenza artificiale, anche generativa, sono consentite in conformità alle disposizioni di cui agli articoli 70-ter e 70-quater*» legge 633/1941.

Mentre la nozione di “*modelli [...] di intelligenza artificiale*” si ricava dall'art. 1 n. 63 *AI Act*<sup>26</sup>, cui fa espresso rinvio l'art. 1, lettera c) della legge (cfr. *supra*, par. 1), lo stesso art. 25, alla lettera a) del primo comma, introduce una previsione integrativa della definizione di “*opere protette*”, di cui all'art. 1, comma 1, legge 633/1941, la cui tutela penale va ora integrata con la complessa disciplina in esame, in quanto nell'ambito delle “*opere dell'ingegno*” – cui viene aggiunta la qualifica distintiva dell'aggettivo “*umano*” – vengono ricondotte anche quelle «*create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del lavoro intellettuale dell'autore*».

In sintesi, tali nuove disposizioni riflettono la consapevolezza che lo sviluppo dei sistemi di intelligenza artificiale e dei relativi modelli generali richiede, da un lato, una disponibilità sempre maggiore, a livello globale, di tutto quanto reperibile in rete, con compressione dei diritti soggettivi degli autori (e non solo); dall'altro, un adeguamento estensivo della stessa nozione di “*opera dell'ingegno*”, che si può realizzare *anche* con l'ausilio di detti sistemi e modelli (sinteticamente ricondotti al concetto inadeguato di “*strumenti*”), che non escludano comunque il contributo *creativo* dell'intelligenza umana,

---

<sup>26</sup> Questa la complessa definizione di “*modello di IA per finalità generali*”: «*un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato [da] una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato*».

con conseguente riconoscimento della necessità di garantirne la tutela penale, nelle nuove condizioni determinate dallo sviluppo tecnologico.

L'interazione profonda che dunque si stabilisce (e si riconosce) fra l'attività intellettuale dell'uomo e l'attività riferibile ai sistemi di intelligenza artificiale, pur con tutte le incertezze che vengono in rilievo in questo contesto, dimostra che essi non sono affatto meri "*strumenti di ausilio*" all'attività creativa riferibile all'uomo soltanto, vista la loro operatività relativamente autonoma, espressa nella loro stessa definizione (cfr. *supra* par. 3.1, nota 12) e che trova riscontro nel fatto che sono "autorizzati" essi stessi a reperire in rete dati e materiali con cui si "addestrano" e si sviluppano ulteriormente.

Quale ultima notazione, non si può non sottolineare che la novella esaminata si occupa dei soli profili della tutela del diritto d'autore, mentre rimane aperta la questione, già emersa, delle possibili violazioni della disciplina posta a tutela dei dati personali. Manca infatti ad oggi una chiara base giuridica che legittimi l'attività di estrazione di dati e testi, a fronte delle garanzie stabilite nel regolamento (UE) 2016/679 (c.d. GDPR), oltre che nel nostro Codice *privacy*: tanto che già in due casi il nostro Garante ha dichiarato la illiceità di simili condotte<sup>27</sup>.

L'art. 9 della legge, rubricato "*Disposizioni in materia di trattamento di dati personali*", riguarda infatti soltanto quelli trattati in ambito sanitario e di ricerca e sperimentazione scientifica.

Sarebbe stato invece auspicabile che, quantomeno nell'ambito delle deleghe legislative previste dall'art. 24, di cui si dirà, vi fosse stata una disposizione che consentisse di colmare questa grave lacuna, essendo necessaria una fonte primaria in materia, per la riserva di legge che va rispettata, sia per ogni limitazione di diritti fondamentali, sia per la disciplina di elementi normativi da cui dipenda l'applicazione di norme penali<sup>28</sup>.

#### 4. Le circostanze aggravanti.

Accanto ai due nuovi reati appena esaminati, la legge introduce un articolato sistema di circostanze aggravanti, che si possono applicare sia a qualsivoglia reato, nel caso dell'aggravante comune prevista dal nuovo n. 11-*undecies*<sup>29</sup> che si aggiunge

---

<sup>27</sup> Si rinvia agli interventi del Garante del 10.2.2022 e del 17.5.2023, reperibili al sito dell'Autorità ([www.gpdp.it](http://www.gpdp.it)), opportunamente segnalati da B. FRAGASSO, *Profili penalistici*, cit., par. 6.2., nota 34.

<sup>28</sup> Tali rilievi critici sono stati già da me sviluppati con riferimento agli artt. 7, 8 ed in specie 9 del testo del d.d.l. approvato dal Governo il 23.4.2024 (A.S. 1146 Senato della Repubblica), poi definitivamente approvati con poche modifiche, per cui si demanda a un decreto del Ministero della salute la concreta disciplina del trattamento di dati anche "*particolari*" (ai sensi dell'art. 9 GDPR) «*per finalità di ricerca e sperimentazione anche tramite sistemi di intelligenza artificiale e machine learning*» (cfr. L. PICOTTI, *Sanità digitale*, cit., par. 2.1, p. 417 s., e par. 3.3.1, p. 421 s.).

<sup>29</sup> La legge prevedeva originariamente il numero "11-*decies*", peraltro nelle more attribuito alla circostanza aggravante introdotta dall'art. 11, comma 1, D.L. 11 aprile 2025, n. 48, convertito dalla L. 9 giugno 2025, n. 80 (c.d. decreto sicurezza): per cui è stato poi corretto in "11-*undecies*" dal Comunicato 17 ottobre 2025, pubblicato nella G.U. 17 ottobre 2025, n. 242.

all'esteso elenco delle circostanze aggravanti comuni di cui all'art. 61 comma 1 c.p., collocato nella parte generale del codice, sia da riferire solo a tre altri specifici reati, indicati dalle disposizioni in esame.

#### 4.1. La nuova circostanza aggravante comune (art. 61 n. 11-undecies c.p.).

Quanto all'aggravante comune, che comporta l'aumento della pena edittale fino ad un terzo, è formulata in termini relativamente complessi, perché non si limita a richiedere che «il fatto sia commesso **mediante** sistemi di intelligenza artificiale», come era previsto nell'originaria formulazione (per cui comunque non si applica se il reato è invece in danno di essi<sup>30</sup>), ma inserisce ulteriori requisiti alternativi, ed in particolare che «per la loro natura o modalità di utilizzo» abbiano costituito «mezzo insidioso»; oppure abbiano «ostacolato la pubblica o la privata difesa»; od infine abbiano «aggravato le conseguenze del reato».

Si tratta di elementi selettivi, che devono essere accertati non senza difficoltà probatorie dal giudice penale per applicare l'aggravamento di pena, ma che in parte potrebbero duplicare od essere assorbiti da specifici elementi di varie fattispecie incriminatrici che vengano in rilievo.

Ad esempio, per quel che riguarda il “mezzo insidioso”, l'aggravante si può sovrapporre agli “artifici e raggiri” costitutivi del reato di truffa (ex art. 640 c.p.), applicabile se vi sia un'interazione con la vittima; ovvero all'“alterazione del funzionamento” di un sistema informatico od all'“intervento senza diritto [...] su dati, informazioni o programmi”, che integrano la frode informatica (ex art. 640-ter c.p.). Ma potrebbero anche essere il mezzo per introdursi “abusivamente” in un sistema informatico protetto (ex art. 615-ter c.p.) ovvero per realizzare “fraudolentemente” intercettazione illecite di comunicazioni informatiche o telematiche (ex art. 617-*quater* c.p.). Ed ancor più nei delitti di falsità in atti pubblici (art. 476 in relazione all'art. 491-*bis* c.p.), la “alterazione” ed ancor più la “contraffazione” potrebbero realizzarsi con l'utilizzo di un sistema di intelligenza artificiale quale “mezzo insidioso”. E così via.

La giurisprudenza e l'elaborazione dottrinale dovranno dunque chiarire come si possa definire il carattere “insidioso” dell'utilizzo di un sistema di intelligenza artificiale, che nei suoi contenuti minimi potrebbe anche essere ravvisato nella semplice mancata informazione all'utente del suo impiego, il cui obbligo è stabilito in generale dall'art. 50 *AI Act*<sup>31</sup>, o che potrebbe presupporre invece un'ulteriore verifica della sua capacità

---

<sup>30</sup> Nelle Raccomandazioni dell'AIDP, contenute nella *Resolution on Traditional Criminal Law Categories and AI*, di cui si è detto *supra* a nota 21, si suggerisce di rafforzare anche la tutela penale dei sistemi di intelligenza artificiale dalle aggressioni che possano subire, data l'importanza della loro funzione, non essendo solo da considerare quale mezzo insidioso per la commissione di reati.

<sup>31</sup> La norma, che occupa l'intero Capo IV dedicato agli “Obblighi di trasparenza per i fornitori e i deployers di determinati sistemi di IA”, prevede che «i fornitori garantiscono che i sistemi di IA destinati a interagire direttamente con le persone fisiche sono progettati e sviluppati in modo tale che le persone fisiche interessate siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo». L'art. 13,

“ingannatoria” a danno della persona offesa, peraltro non espressamente richiesta, come è invece prevista espressamente nel nuovo delitto di cui all’art. 612-*quater* c.p. (cfr. *supra*, par. 3.1.).

L’interpretazione del requisito dell’“ostacolo” alla pubblica e alla privata difesa potrebbe valorizzare l’elaborazione relativa all’analoga formulazione della circostanza aggravante di cui al n. 5 dello stesso art. 61 c.p. In questa vi è però un espresso richiamo anche alle «*circostanze di tempo, di luogo o di persona, anche in riferimento all’età*» che devono essere «*tali da ostacolare la pubblica o privata difesa*». Per cui si rendono necessari specifici adattamenti interpretativi che considerino la commissione del reato nel diverso ambiente tecnologico e “virtuale” in cui si deve applicare la nuova aggravante.

Un simile ragionamento potrebbe valere anche per l’aggravamento delle conseguenze del reato, che già costituisce, in sostanza, un’altra circostanza aggravante comune, prevista dal n. 8 del medesimo art. 61 c.p.

In entrambi i casi, l’elemento che sembra supportare la maggior offensività riconosciuta con l’aggravamento di pena è dato dalla portata espansiva e diffusiva, in tempi immediati, dei delitti commessi con l’impiego di sistemi di intelligenza artificiale, di cui potrebbe sfuggire la stessa percezione da parte della vittima. E le loro conseguenze possono così colpire enti e persone in un numero indeterminato ed improvviso, eludendo, più che “ostacolando”, le possibilità di difesa e diffondendosi potenzialmente a livello globale in tutta la rete.

Nonostante questi rilievi, non si comprende del tutto la necessità di inserire i requisiti in esame all’interno della nuova circostanza aggravante, imperniata sull’uso di sistemi di intelligenza artificiale, visto che sarebbe sempre stato possibile un suo concorso con le circostanze aggravanti menzionate, che la formulazione in esame invece scongiura, in ossequio al principio di specialità.

#### 4.2. Le circostanze aggravanti speciali introdotte nel codice e nella legislazione speciale.

Quanto alle tre circostanze aggravanti speciali, che determinano un aumento di pena in modo autonomo, maggiore di un terzo, per il reato cui ciascuna si riferisce, va premesso che rientrano nella disciplina delle “*circostanze ad effetto speciale*” di cui all’art. 63, comma 3, c.p., con ogni conseguenza in caso di concorso. Esse consistono tutte nel mero «*impiego di sistemi di intelligenza artificiale*», non essendo per queste richiesti (per ragioni che sfuggono) i requisiti aggiuntivi presenti invece nella circostanza aggravante comune, di cui si è appena detto.

Si tratta di ipotesi selezionate con criteri che non consentono neppure di individuare una chiara linea di politica criminale, vista la diversità dei beni giuridici che vengono in rilievo e la diversità di struttura delle condotte cui accedono.

---

comma 2, della legge, dispone a sua volta un tassativo obbligo di informazione in capo a chi esercita professioni intellettuali.

**4.2.1.** Nella prima ipotesi codicistica, riferita al delitto di “*Attentato contro i diritti politici del cittadino*” (art. 294 c.p.), che si colloca quale unica fattispecie del Capo III nel Titolo I della Parte speciale del codice, dedicato ai “*delitti contro la personalità dello Stato*”, si riflette la preoccupazione per gli effetti manipolativi che i sistemi di intelligenza artificiale possono determinare sull’esercizio dei diritti politici.

Il fatto base consiste nell’impedire il loro esercizio «*in tutto od in parte*», ovvero «*determina[re] taluno a esercitar[li] in senso difforme dalla sua volontà*» attraverso le tre modalità tipiche della «*violenza, minaccia o inganno*» di cui al comma 1.

La circostanza aggravante in esame si riferisce invece espressamente alla (sola) ipotesi dell’“*inganno*”, se “*posto in essere*” mediante detti sistemi.

Evidentemente il legislatore non ritiene sufficientemente fronteggiato dal nuovo delitto di cui all’art. 612-*quater* c.p., sopra esaminato, il c.d. *deep fake* che – al di là delle ipotesi di offesa alla sfera dell’identità ed autodeterminazione in ambito sessuale (detto anche *porn deep fake*, di cui si è detto) – colpisca la stessa regolarità dei processi elettorali democratici, offendendo il libero esercizio dei diritti politici individuali. La maggior gravità sanzionatoria (pena della reclusione da 2 a 6 anni, per vero non molto maggiore di quella di cui all’art. 612-*quater* c.p.), accanto alla procedibilità d’ufficio, esprime quindi la maggior importanza del bene giuridico protetto, che si colloca in una dimensione pubblica di difesa degli stessi meccanismi decisionali del sistema democratico, contro la possibilità di un inquinamento subdolo del dibattito pubblico e del corretto gioco elettorale, che può anche provenire dall’esterno della nazione. Fermo restando che tale difesa non può certo essere circoscritta al – quasi solo simbolico – strumento punitivo, difficilmente in grado di fronteggiare e, soprattutto, prevenire i preoccupanti fenomeni in esame.

**4.2.2.** Le altre due circostanze aggravanti riguardano delitti collocati fuori del codice penale, ed in particolare l’aggiotaggio c.d. bancario e societario, di cui all’art. 2637 c.c., e l’aggiotaggio c.d. finanziario o manipolazione del mercato, di cui all’art. 185 TUF, relativo ai mercati regolamentati. Si tratta di fatti di reato aventi una struttura identica, non lontana dal modello originario dell’aggiotaggio comune di cui all’art. 501 c.p. (al quale peraltro non è stato previsto che si applichi un’aggravante analoga), che si realizzano con la diffusione di notizie false (c.d. aggiotaggio informativo) o, in alternativa, con operazioni simulate od altri artifici (c.d. aggiotaggio operativo), che siano «*concretamente idonei a provocare una sensibile alterazione dei prezzi*»<sup>32</sup>. La ragione dell’aggravamento sanzionatorio (fra un minimo di 2 ed un massimo di 7 anni di reclusione ed, in relazione al solo art. 185 TUF, anche da 25.000 a 6 milioni di euro di multa) si correla all’esigenza di rafforzare la tutela penale delle regolari contrattazioni dei titoli, in specie in borsa, di fronte all’utilizzo sempre più diffuso di sistemi di intelligenza artificiale nel c.d. *trading* algoritmico, grazie a cui – per fortissime ragioni di rapidità ed efficacia – le decisioni di acquisto e vendita sui diversi mercati, ed in specie

---

<sup>32</sup> Gli “abusi di mercato” in cui rientrano i delitti in esame, trovano più ampie definizioni sia quali illeciti amministrativi nel regolamento (UE) 2014/596 (c.d. MAR), artt. 8, 10 e 12, sia quali illeciti da sanzionare penalmente nella direttiva 2014/54/UE, artt. 3-5.

in quelli finanziari, vengono operate direttamente ed in tempo reale da tali sistemi, secondo strategie stabilite in generale dagli operatori che se ne avvalgono, ma poi concretamente poste in essere ed eseguite con notevoli margini di autonomia dai sistemi stessi<sup>33</sup>.

L'aggravamento di pena che sarebbe così perseguito dal legislatore, rispetto a pene edittali già elevate, è però da criticare, sia sul piano tecnico-normativo, sia sotto il profilo degli elementi oggettivi e soggettivi.

Sotto il primo profilo, è già stato osservato dai primi commentatori<sup>34</sup>, che l'art. 39 legge 28 dicembre 2005 n. 262 aveva precedentemente innalzato ad un livello superiore a quella oggi stabilita con l'aggravante speciale in esame la pena edittale dell'art. 185 TUF, portandola alla reclusione da 2 a 12 anni. Per cui, paradossalmente, la nuova disposizione in commento non solo non comporta alcun effetto aggravatore, ma anzi determina una necessaria riduzione della stessa pena base, che non può superare quella stabilita dalla nuova circostanza. Al riguardo, dovrebbe valere infatti il recente orientamento della Cassazione a Sezioni unite<sup>35</sup> secondo cui, in un caso analogo, deve intendersi abrogata per incompatibilità, dalla norma successiva più favorevole, quella precedente che aveva disposto l'aumento.

Le disposizioni in esame portano in ogni caso, sul piano oggettivo, ad una generalizzata applicazione dell'aggravamento di pena, stante il normale e diffuso, ma di per sé anche legittimo, impiego di sistemi di intelligenza artificiale nelle contrattazioni di mercato e di borsa. Per cui ogni "alterazione" dei prezzi, da ricondurre a fatti qualificabili come aggio, verrebbe automaticamente anche aggravata, non richiedendosi l'accertamento dei requisiti aggiuntivi, previsti solo dalla circostanza aggravante comune di cui si è detto, che rimandano alla «*loro natura o modalità di utilizzo*» o che abbiano costituito «*mezzo insidioso*» od «*ostacolo la pubblica o la privata difesa*», od infine abbiano «*aggravato le conseguenze del reato*».

Sul piano soggettivo, infine, avvenendo per regola generale l'imputazione delle circostanze aggravanti a titolo di colpa, *ex art. 59 comma 2 c.p.*, dato che si applicano anche se l'agente le ignora per colpa o le ritiene inesistenti per errore dovuto a colpa, *non occorre* che egli abbia una specifica rappresentazione e volizione non tanto dell'impiego in sé, normalmente legittimo e voluto, di tali sistemi, ma del fatto che *mediante* gli stessi si realizzino i reati in questione.

In altri termini, la circostanza aggravante opera anche se l'operatore non abbia consapevolmente voluto che il sistema di intelligenza artificiale potesse essere strumento per la diffusione di notizie false o per la realizzazione di operazioni simulate od altri artifici, idonei a provocare quella «*sensibile alterazione dei prezzi*» da differenziare dalle

---

<sup>33</sup> In argomento basti qui il rinvio a F. CONSULICH, *Il nastro di Mobius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato*, in *Banca, borsa, tit. cred.*, 2/2018, p. 195 s.; e da ultimo alla tesi dottorale di A. BACCIN, *Algoritmizzazione dei mercati finanziari, abusi di mercato e criteri di imputazione penale all'epoca delle strategie High-Frequency Trading*, Università di Verona, 2025, con aggiornate indicazioni bibliografiche.

<sup>34</sup> F. MUCCIARELLI, [Intelligenza artificiale e condotte manipolative su strumenti finanziari: una nuova aggravante con effetto attenuante](#), in *questa Rivista*, 17 ottobre 2025.

<sup>35</sup> Cass., Sez. un. 27 aprile 2023, n. 17615.

normali oscillazioni del mercato, dipendenti dal legittimo gioco della domanda e dell'offerta: per cui l'aggravamento si deve applicare per aver semplicemente ignorato ("per colpa") che questo avvenisse.

## 5. Sulle norme di delegazione in materia penale.

L'art. 24, collocato senza adeguata evidenza nel contesto del Capo III, dedicato in generale alla "strategia nazionale", alle "autorità nazionali" e ad "azioni di promozione", contiene in realtà un ampio sistema di deleghe legislative al governo in materia di intelligenza artificiale, fra cui va in questa sede menzionata quella ad emanare «uno o più decreti legislativi» finalizzati ad «adeguare e specificare la disciplina dei casi di realizzazione e di impiego **illeciti** di sistemi di intelligenza artificiale» (comma 3, grassetto aggiunto).

È una norma scarsamente determinata nell'oggetto, non essendo precisati i parametri per stabilire quali potrebbero essere gli ambiti ed i casi di "realizzazione" ed "impiego" genericamente "illeciti" dei sistemi in esame, né a che tipologie di illeciti si riferisca il legislatore delegante.

Solo nel successivo comma 5 vi sono importanti, pur se non sufficienti, specificazioni, che riguardano (anche) la materia penale.

5.1. Alla lettera d) è prevista per vero una delega relativa alla *responsabilità civile*, che enuncia alcuni criteri e principi da rispettare per la sua attuazione, mentre alla lettera e) la delega concerne la «regolazione dell'utilizzo di sistemi di intelligenza artificiale nelle indagini preliminari», con assenza invece di una precisa indicazione dei criteri da seguire, salvi alcuni principi guida da rispettare, di carattere molto generale, quali le «*garanzie inerenti al diritto di difesa e ai dati personali dei terzi*» ed i «*principi di proporzionalità, non discriminazione e trasparenza*».

Le altre lettere, che contengono deleghe in materia di diritto penale sostanziale, sono ancora più carenti di precisione nel delimitarne l'oggetto e, soprattutto, prive di criteri direttivi e principi guida, collidendo *prima facie* con il disposto dell'art. 76 Cost., su cui si tornerà.

Le deleghe che riguardano il diritto penale sostanziale si possono distinguere in tre nuclei.

5.2. Alla lettera a) del menzionato comma 5 si prevede che debbano essere introdotti «**strumenti**, anche **cautelari**, finalizzati a inibire la diffusione e a rimuovere contenuti generati illecitamente anche con sistemi di intelligenza artificiale», e che questi siano «*assistiti da un sistema di sanzioni efficaci, proporzionate e dissuasive*», fra cui potrebbero rientrare anche sanzioni penali, benché non siano prescritte.

È evidente l'ampio spazio discrezionale così garantito al legislatore delegato, sia nella scelta e disciplina di siffatti "strumenti", che potrebbero essere di natura civile, penale o amministrativa, e possono, o forse anzi debbono, essere altresì "cautelari", data l'urgenza degli interventi nell'ambito digitale, sia nella scelta della tipologia ed entità

delle sanzioni che devono “*assisterli*”, per cui non è neppure stabilito se debbano essere penali.

5.3. Nella successiva lettera b) la delega riguarda l’introduzione di «*autonome fattispecie di reato punite a titolo di dolo o di colpa*» incentrate su condotte omissive, per la mancata adozione o il mancato adeguamento di misure di sicurezza da osservare per la produzione, messa in circolazione e utilizzo professionale di sistemi di intelligenza artificiale, da cui possa derivare un «*pericolo concreto per la vita o l’incolumità pubblica o individuale o per la sicurezza dello Stato*».

La previsione è importante, riflettendo nell’ambito penale quell’approccio basato sulla valutazione e prevenzione del rischio inerente alla produzione ed utilizzazione di questi sistemi, che innerva tutta la disciplina vigente, ed in specie quella europea<sup>36</sup>.

Tuttavia, resta del tutto in sospeso la scelta fra reati “*dolosi o colposi*”, da cui dipende anche la rispettiva gravità, da correlare alla natura dei beni giuridici che meritano protezione, che sono solo genericamente e riduttivamente indicati (*vita, incolumità pubblica o individuale, per la sicurezza dello Stato*), non toccando tutto l’importante ambito degli altri diritti della persona e della collettività, che possono essere offesi dall’impiego di sistemi di intelligenza artificiale.

5.4. Alla lettera c), la delega ha poi un oggetto ancor più generale, anzi generico, riguardando la «*precisione dei criteri di imputazione della responsabilità penale delle persone fisiche*», oltre che quella «*amministrativa degli enti per gli illeciti inerenti a sistemi di intelligenza artificiale*».

Se, da un lato, la previsione riconosce che occorre un intervento legislativo per stabilire i presupposti ed i criteri di imputazione della responsabilità penale per reati commessi tramite sistemi di intelligenza artificiale, rispetto a cui occorre risalire alle persone umane, fisiche o giuridiche, che “*stanno dietro*” di essi, dalla fase della ideazione, a quelle della produzione, commercializzazione, messa a disposizione ed utilizzazione finale, dall’altro lato i parametri da seguire per stabilire la responsabilità penale, che deve essere necessariamente “*personale*” e, dunque, anche soggettivamente colpevole (*ex art. 27 commi 1 e 3 Cost.*)<sup>37</sup>, per fatti in cui i sistemi di intelligenza artificiale assumono funzioni decisionali rilevanti, con crescenti spazi di autonomia, sono molto controversi ed oggetto di un acceso dibattito in dottrina, non solo a livello nazionale<sup>38</sup>.

Per cui appare fuorviante la testuale affermazione, secondo cui detti “*criteri di imputazione*” dovrebbero essere (soltanto) “*precisati*”, senza che sia chiara quale sia la

---

<sup>36</sup> In argomento si veda di recente L. D’AMICO, *La misura della (im)prevedibilità. Modelli d’imputazione della responsabilità al tempo dell’intelligenza artificiale*, Napoli, 2025, in specie Parte II, cap. 2, p. 219 s.; volendo anche L. PICOTTI, *Categorie tradizionali del diritto penale*, cit., in specie par. 3.3.1, p. 9 s. sull’imputazione oggettiva e par. 3.3.2.2, p. 14, sulla colpa.

<sup>37</sup> Per tale imprescindibile esigenza si rinvia per tutti alle citate Raccomandazioni elaborate all’esito dei lavori dell’AIDP (*supra*, nota 29).

<sup>38</sup> In argomento, oltre che ai lavori e alle già citate Raccomandazioni dell’AIDP di cui alla nota 29, nella vasta letteratura nazionale ed internazionale si rimanda al quadro tracciato da A. GIANNINI, *Criminal Behavior* cit., con ampie indicazioni bibliografiche.

base di riferimento<sup>39</sup> e non essendo certo sufficiente l'unica indicazione suggerita, di «ten[er] conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente».

Elemento certo importante, che si collega al principio di sorveglianza umana contenuto anche nell'art. 14 *AI Act*, ma che (come riconosce la stessa locuzione: «tenuto conto...») va precisamente definito in relazione anche ad altri pregnanti parametri fondativi, riconducibili alle diverse competenze e funzioni della “catena di valore” dei vari soggetti responsabili che “stanno dietro” l'intelligenza artificiale, richiamati del resto anche dall'art. 25 *AI Act*.

5.5. Infine, per quanto riguarda la responsabilità “da reato” degli enti, semplicemente richiamata dalla lettera c) del comma 5 in esame, come materia parimenti oggetto di delega accanto a quella penale delle persone fisiche, manca *qualsiasi indicazione* di specifici “criteri direttivi”, non potendo direttamente valere anche per essi il richiamo a «tener conto» del «livello effettivo di controllo da parte dell'agente», evidentemente riferito alla persona fisica, mentre l'imputazione all'ente giuridico si riferisce alla sua organizzazione collettiva.

In effetti, proprio la funzione spiccatamente preventiva, che innerva la disciplina della responsabilità da reato dell'ente, dovrebbe rappresentare la prospettiva più idonea per implementare l'approccio basato sul *risk assessment*, da specificare con relativi obblighi, oneri e conseguenze<sup>40</sup>.

In argomento è stato giustamente evidenziato che già la *AI Act* europeo prevede un forte apparato sanzionatorio, dotato di pesanti sanzioni pecuniarie amministrative, applicabili agli enti<sup>41</sup>, cui la legge nazionale dovrà “adeguarsi”, non certo sostituirle o renderle inapplicabili.

Il problema non è in effetti quello di evitare un sistema di doppio binario, che è presente in tanti altri settori (a partire dalla materia della protezione e disciplina dei dati personali, fino a quella dei mercati finanziari e del diritto d'autore), e che non è necessario escludere, secondo la giurisprudenza ormai consolidata della Corte di Giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo, data la diversità di competenze e la rapidità di interventi normativi ed amministrativi riconducibili alle Autorità interessate, purché sia rispettato (soprattutto) il limite delle proporzioni<sup>42</sup>.

Si tratta piuttosto di valorizzare più in dettaglio la prospettiva della prevenzione degli specifici reati in esame mediante un'adeguata valutazione preventiva e dinamica

<sup>39</sup> Fra i primi commenti c'è chi ha ritenuto che il termine “precisare” dovrebbe significare una limitazione dell'ambito di responsabilità (B. FRAGASSO, *Profili penalistici*, par. 8.3). Ma non vi è un effettivo supporto lessicale, né logico, ad una tale interpretazione, visto che il verbo “precisare” indica soltanto un'esigenza di specificità, che può ed anzi dovrebbe emergere anche per fondare od estendere la responsabilità, non soltanto per limitarla.

<sup>40</sup> Cfr. ancora le Raccomandazioni dell'AIDP citate a nota 29, in specie par. 4, punto 16. Volendo si veda anche L. PICOTTI, *Categorie tradizionali*, cit., par. 3.5, p. 16 s.

<sup>41</sup> B. FRAGASSO, *Profili penalistici*, par. 9.

<sup>42</sup> Nella vastissima letteratura in argomento, basti qui il rinvio a M. SCOLETTA, [Il principio di ne bis in idem e i modelli punitivi a doppio binario](#), in *Dir. pen. cont. – Riv. trim.*, 4/2021, 180 s.

dei rischi e una corrispondente organizzazione dell'ente, di grande rilievo per il collegamento strutturale che ha con la produzione, l'implementazione e l'utilizzazione di sistemi di intelligenza artificiale. Tanto che si è già valorizzata l'autonomia della responsabilità dell'ente rispetto a quella delle persone fisiche che nel suo seno operano e l'insufficienza, però, dell'elenco di reati c.d. presupposto<sup>43</sup>, che caratterizza ancora oggi il decreto legislativo 231 del 2001.

5.6. Alla lettera f) del comma 5 dell'art. 24 in esame sono, infine, previste deleghe per il "coordinamento" e la "razionalizzazione" della normativa sia sostanziale che processuale vigente, da realizzare «in conformità ai principi e criteri enunciati», per vero ben difficili da rinvenire. Per cui se tali deleghe sono ancor più generiche delle altre appena esaminate, appaiono precisabili solo in futuro, alla stregua della normativa delegata che verrà emanata e sarà da coordinare e razionalizzare nell'ambito del sistema penale.

5.7. Conclusivamente, in questa sede non ci si può esimere dal sollevare forti perplessità per lo scarso rispetto delle condizioni, che l'art. 76 Cost. pone tassativamente al Parlamento legislatore, per la delegazione della sua funzione al Governo.

Infatti, non solo essa deve essere conferita per un "tempo limitato" (in questo caso 12 mesi, che appare rispettoso di detto limite), ma anche riguardare "oggetti definiti" e soprattutto contenere "principi e criteri direttivi", cui il legislatore delegato deve attenersi: condizioni queste ultime due che non appaiono rispettate, o almeno non lo sono pienamente, per le ragioni via via evidenziate e del resto fatte presenti in sede di lavori parlamentari sia dal Comitato per la legislazione, sia dalla Prima Commissione permanente della Camera dei deputati<sup>44</sup>.

La Corte costituzionale dovrà, dunque, esercitare un attento doppio scrutinio di legittimità sui decreti legislativi che verranno emanati: il primo riguardante il rispetto delle condizioni poste dall'art. 76 Cost. alla legge parlamentare di delegazione, il secondo riguardante il rispetto dei principi e criteri direttivi da essa posti da parte del legislatore delegato, quando interverrà.

E tale scrutinio dovrà essere tanto più rigoroso, in quanto si tratta di delega conferita in materia penale, in cui vige un principio di stretta legalità, per la riserva assoluta di legge stabilita dall'art. 25 comma 2 Cost., che ha portato autorevole dottrina a ritenere addirittura non conforme ad essa *qualsiasi* produzione normativa che non

---

<sup>43</sup> Sia consentito ancora il rinvio a L. PICOTTI, *Categorie tradizionali*, cit., 3.5, p. 17.

<sup>44</sup> Al riguardo, è sorprendente e fortemente censurabile il fatto che non si siano considerati gli specifici rilievi critici che erano stati espressi sia dal "Comitato per la legislazione", sia dalla "I Commissione permanente (Affari costituzionali)" durante l'esame del d.d.l. trasmesso dal Senato il 20 marzo 2025 e divenuto il numero A.C. 2316-A Camera dei Deputati. In essi si era chiaramente e motivatamente segnalata la necessità che, specie in materia penale, le deleghe legislative al Governo contenessero «criteri direttivi e principi configurati in modo assai preciso», con puntuali richiami alle molteplici statuizioni della Corte costituzionale al riguardo. Ma il Parlamento ha proceduto all'approvazione in entrambi i rami, senza rispetto delle prescrizioni costituzionali puntualmente evidenziate.

provenza esclusivamente dal Parlamento, in quanto unico organo rappresentativo anche delle minoranze e pienamente espressivo della sovranità popolare<sup>45</sup>.

## 6. Osservazioni conclusive.

Un breve bilancio provvisorio sui contenuti penali della nuova legge in commento consente di apprezzare, da un lato, la tempestività dell'intervento normativo, diretto ad offrire un quadro di maggior certezza, e non solo di sicurezza, a cittadini ed enti, nel complesso quadro di veloce sviluppo della materia e del relativo mercato.

Ma dall'altro non poche sono le incongruenze rilevate, a partire da una impostazione già censurata come "panpenalistica" che punta molto sull'aggravamento delle sanzioni, mediante nuove circostanze comuni e speciali, aventi un valore soprattutto simbolico di messaggio politico, oltre alla creazione di nuovi reati, mentre il diritto penale dovrebbe restare l'ultima *ratio* di tutela e governo della materia, che dovendosi intervenire a monte con altri strumenti, a partire da una dettagliata promozione di regole cautelari e standard di sicurezza nei diversi settori (dalle auto a guida autonoma, all'impiego dell'intelligenza artificiale e della robotica nella medicina, nelle contrattazioni di borsa, nella domotica, e così via).

Dunque, questo primo passo, certo importante per la sua dimensione strutturale, richiede ancora un lungo ed approfondito impegno di elaborazione sotto il profilo penalistico, soprattutto in vista dell'esercizio delle deleghe legislative, carenti di criteri e principi direttivi, per cui dovranno stimolarsi e valorizzarsi i necessari contributi di organismi ed enti competenti, e non da ultimo della dottrina.

---

<sup>45</sup> Si veda già F. BRICOLA, *Teoria generale del reato*, in *Noviss. Dig. It.*, 1972, p. 10 s.; nonché G. MARINUCCI, E. DOLCINI, *Corso di diritto penale. 1. Le norme penali: fonti e limiti di applicabilità. Il reato: nozione, struttura e sistematica*, 3<sup>a</sup> ed., Milano 2001, § 4.1.5.6, in specie p. 50.