



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

© Copyright 2026 - G. GIAPPICHELLI EDITORE - TORINO

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.



UNIVERSITÀ
DEGLI STUDI
DI MILANO

Stampa: Stampatre s.r.l. - Torino

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633.

Le fotocopie effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da CLEARedi, Centro Licenze e Autorizzazioni per le Riproduzioni Editoriali, Corso di Porta Romana 108, 20122 Milano, e-mail autorizzazioni@clearedi.org e sito web www.clearedi.org.

INDICE

	<i>pag.</i>
<i>Elenco degli Autori e delle Autrici</i>	XXIX
<i>Presentazione</i>	XXXIII

INTRODUZIONE

LA REGOLAZIONE DIGITALE EUROPEA NEL CONTESTO DELLE RECENTI TRASFORMAZIONI GEOPOLITICHE

<i>Francisco Balaguer Callejón</i>	1
1. I paradossi della regolazione dell'IA	1
2. Quando il potere digitale incontra quello geopolitico	7
3. Una nuova architettura politica europea per l'attuazione della regolazione digitale	10
<i>Riferimenti bibliografici</i>	15

INTRODUZIONE

L'INTELLIGENZA ARTIFICIALE E LA SFIDA REGOLATORIA SUL DUPLICE VERSANTE, EUROPEO E NAZIONALE

<i>Marilisa D'Amico</i>	17
1. L'IA tra rischi e prospettive per la tutela dei diritti fondamentali	17
2. Regolamentare l'IA nel prisma dei principi costituzionali in una prospettiva multilivello	21
3. La legge n. 132/2025: la prospettiva italiana letta nell'ottica di una strategia di sviluppo	23
4. La promozione dell'innovazione tecnologica senza perdere la "bussola" del costituzionalismo	25
<i>Riferimenti bibliografici</i>	27

INTRODUZIONE

IL REGOLAMENTO EUROPEO E LE PROFESSIONI LEGALI.
LA RIVOLUZIONE DELL'IA E LA SFIDA PER IL DIRITTO
E L'AVVOCATURA

<i>Antonino La Lumia</i>	29
1. Premessa	29
2. Opportunità e rischi dell'Intelligenza Artificiale per l'Avvocatura	30
3. Il quadro normativo e valoriale: tecnologie e controllo umano	31
4. Il nuovo approccio per l'Avvocatura e per le professioni legali	33
5. L'Avvocatura come garante di diritti nella società digitale	34

PARTE I

IL REGOLAMENTO (UE) 2024/1698

SEZIONE I

LE COORDINATE GENERALI

CAPITOLO I

OGGETTO E AMBITO DI APPLICAZIONE DEL
REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE

Commento agli artt. 1, 2 e 3

<i>Juan Francisco Sánchez Barrilao</i>	43
1. Introduzione: che cosa intendiamo per IA e come regolamentarla?	43
2. Oggetto di regolazione dell'AI Act	45
2.1. Il mercato europeo dell'IA	46
2.2. Contenuti dell'AI Act	46
2.3. L'IA come prodotto affidabile inserita in un mercato affidabile	47
3. Concetto di IA ai fini dell'AI Act	47
3.1. Positivizzazione del concetto di IA nell'AI Act	48
3.2. Che cosa intende l'AI Act per IA?	50
3.3. Linee guida della Commissione in merito al concetto di IA	50
3.4. L'IA ad uso generale	51
3.5. Altri concetti dell'AI Act	53
4. Portata materiale della regolazione dell'AI Act	53

	<i>pag.</i>
4.1. IA e scienza	54
4.2. IA, difesa e sicurezza nazionale	54
4.3. IA a codice aperto	56
4.4. Altri casi esclusi, parzialmente o totalmente, oppure semplicemente spostati dall'ambito regolato dall'AI Act	57
5. Considerazioni finali	58
<i>Riferimenti bibliografici</i>	59

CAPITOLO II

TITOLARITÀ E DIRITTI NEL AI EUROPEAN ACT: UTENTI E FORNITORI

Commento agli artt. 2 e 3

Augusto Aguilar Calahorra

61

1. I soggetti di diritto nel Regolamento	61
1.1. Gli artt. 2 e 3 del Regolamento	63
1.2. I soggetti del Regolamento	65
1.3. Le imprese e i fabbricanti quali titolari del processo di produzione normativa	70
2. Soggetti e oggetti del diritto dell'Unione Europea	70
2.1. I soggetti di diritto nell'UE	71
2.2. Gli oggetti del traffico giuridico	74
3. Conclusioni. La trasformazione del soggetto in "oggetto" nel Regolamento sull'intelligenza artificiale	77
<i>Riferimenti bibliografici</i>	78

CAPITOLO III

ISTRUZIONE E INNOVAZIONE NEL REGOLAMENTO (UE) 2024/1689

Commento agli artt. 4 e 57-63

Luis Fernando Martínez Quevedo

81

1. Introduzione	81
2. Educazione	82
3. Innovazione	86
4. Conclusioni	90
<i>Riferimenti bibliografici</i>	91

SEZIONE II
DIRITTI E GARANZIE FONDAMENTALI
NEI SISTEMI VIETATI

CAPITOLO IV

LIBERTÀ DI PENSIERO, AUTONOMIA DI VOLONTÀ,
TECNICHE SUBLIMINALI

Commento all'art. 5, par. 1, lett. a)

<i>Nannerel Fiano</i>	95
1. Introduzione	95
2. Le c.d. “macchine ingannevoli”: quali incantesimi?	96
3. L'IA ambigua	97
4. I <i>deepfake</i>	101
5. I principi della Carta coinvolti	102
6. Conclusioni: per il disincanto degli algoritmi	103
<i>Riferimenti bibliografici</i>	104

CAPITOLO V

LA VULNERABILITÀ COME FATTORE DI DIVIETO PER LE
PRATICHE DI IA

Commento all'art. 5, par. 1, lett. b)

<i>Giuseppe Arconzo, Gaia Patarini</i>	105
1. Il divieto di sfruttamento delle vulnerabilità	105
2. I singoli fattori di vulnerabilità previsti dall'art. 5, par. 1, lett. b)	110
3. Le altre condizioni affinché operi il divieto: l'obiettivo di distorcere il comportamento e il danno significativo	113
4. Brevi considerazioni conclusive	115
<i>Riferimenti bibliografici</i>	116

CAPITOLO VI

PUNTEGGIO SOCIALE E PREVISIONE E VALUTAZIONE
DELLA COMMISSIONE DI REATI

Commento all'art. 5, par. 1, lett. c)-d)

<i>Emma Fidenzi</i>	118
1. Premessa	118

	<i>pag.</i>
2. Intelligenza artificiale e <i>social scoring</i>	120
3. Intelligenza artificiale e la valutazione e previsione della commissione di reati	123
4. Conclusioni	127
<i>Riferimenti bibliografici</i>	130

CAPITOLO VII

RICONOSCIMENTO FACCIALE E RICONOSCIMENTO
DELLE EMOZIONI

Commento all'art. 5, par. 1, lett. e)-f)

<i>Marta Lucena Pérez</i>	131
1. Introduzione	131
2. Riguardo al riconoscimento facciale e delle emozioni	133
3. Conclusioni	137
<i>Riferimenti bibliografici</i>	138

CAPITOLO VIII

DIVIETO DI CATEGORIZZAZIONE PER MOTIVI
DI RAZZA, IDEOLOGIA, AFFILIAZIONE, RELIGIONE

Commento all'art. 5, par. 1, lett. g)

<i>Enrique Guillén López</i>	139
1. Questioni generali e metodologiche	139
2. Giustificazione generale del divieto. Implicazioni della categorizzazione di informazioni o categorie sensibili	142
3. Soggetti obbligati dal divieto e soggetti protetti	143
4. Le condizioni del divieto	144
4.1. Attività	144
4.2. Categorizzazione biometrica	145
4.3. Dati biometrici	146
5. L'oggetto della categorizzazione vietata	147
6. L'eccezione	151
<i>Riferimenti bibliografici</i>	153

CAPITOLO IX

IL DIVIETO DI CATEGORIZZAZIONE BIOMETRICA
SULLA BASE DELLA VITA SESSUALE E
DELL'ORIENTAMENTO SESSUALE

Commento all'art. 5, par. 1, lett. g)

Sara Di Giovanni

155

1. Introduzione: le pratiche di IA a rischio inaccettabile nel sistema dell'AI Act 155
 2. L'ambito di applicazione della lett. g): definizioni, oggetto e *ratio* 158
 3. Le inferenze biometriche su vita sessuale e orientamento sessuale: (im)possibilità tecnica e rischi discriminatori 162
 4. Riflessioni conclusive 167
- Riferimenti bibliografici* 168

CAPITOLO X

L'IDENTIFICAZIONE BIOMETRICA REMOTA IN TEMPO
REALE NELLO SPAZIO PUBBLICO

Commento all'art. 5, par. 1, lett. h) e par. 2

Adoración Galera Victoria

170

1. L'AI Act e l'identificazione biometrica 170
 2. Cosa vieta l'art. 5, par. 1, lett. h)? 174
 3. L'eccezione al divieto: cosa, quando e come? 176
 4. Conclusioni 179
- Riferimenti bibliografici* 180

CAPITOLO XI

AUTORIZZAZIONE E SORVEGLIANZA NELL'USO DEI
SISTEMI DI IDENTIFICAZIONE BIOMETRICA REMOTA

Commento all'art. 5, parr. 3-8

Giulia Agrati

182

1. Introduzione 182
 2. Il meccanismo di autorizzazione e il ruolo dell'autorità giudiziaria o autorità amministrativa indipendente 184
 3. Il meccanismo di controllo e il ruolo dell'autorità di vigilanza del mercato e dell'autorità nazionale per la protezione dei dati 190
- Riferimenti bibliografici* 192

SEZIONE III
SISTEMI DI INTELLIGENZA ARTIFICIALE
AD ALTO RISCHIO

A) *Classificazione*

CAPITOLO XII

LA DISCIPLINA DEI SISTEMI DI INTELLIGENZA
ARTIFICIALE AD ALTO RISCHIO SECONDO L'AI ACT

Commento agli artt. 6 e 7

Costanza Nardocci

195

1. L'approccio in base al rischio (e la nozione di rischio) nell'impianto dell'*AI Act* 195
 2. Le categorie e le implicazioni dell'"alto rischio" secondo l'art. 6: un sistema binario derogabile 200
 3. L'art. 6 *AI Act* 203
 - 3.1. Il par. n. 1 e il par. n. 2 (la tipizzazione dei sistemi "ad alto rischio" e l'Allegato III) 203
 - 3.2. Oltre l'Allegato III: l'art. 6, par. n. 3 e le deroghe all'"alto rischio" (*the filter*) 206
 - 3.3. L'inderogabilità del *profiling* nell'art. 6, par. n. 3: dove arriva il GDPR, ma non il diritto anti-discriminatori 207
 4. Soggetti e obbligazioni (*positive*) 210
 - 4.1. Il *provider*, che faccia uso di tecnologie di IA "ad alto rischio" 210
 - 4.2. Tra art. 6 e art. 7: la *Commissione UE*, che implementa ed emenda l'art. 6 e l'Allegato III 212
 5. Per concludere: un approccio soddisfacente? 216
- Riferimenti bibliografici* 218

CAPITOLO XIII

I SISTEMI AD ALTO RISCHIO IN AMBITO DI BIOMETRIA
E INFRASTRUTTURE CRITICHE

Commento all'Allegato III, parr. 1-2

Amalia Lozano España

220

1. Introduzione 220
2. La biometria 223

	<i>pag.</i>
2.1. I sistemi di identificazione biometrica remota <i>ex post</i>	225
2.2. Categorizzazione biometrica basata su attributi sensibili	226
2.3. Sistemi destinati al riconoscimento delle emozioni	227
3. I sistemi ad alto rischio relativi alle infrastrutture critiche	228
4. Obblighi principali in presenza di un'IA "ad alto rischio" quale la biometria e le infrastrutture critiche	231
5. Conclusione	231
<i>Riferimenti bibliografici</i>	232
CAPITOLO XIV	
I SISTEMI AD ALTO RISCHIO IN MATERIA DI ISTRUZIONE ED OCCUPAZIONE	
Commento all'Allegato III, parr. 3-4	
<i>Antonio Pérez Miras</i>	233
1. A mo' d'introduzione: i sistemi ad alto rischio e l'Allegato III	233
2. I sistemi di IA ad alto rischio sull'istruzione e sulla formazione professionale	239
3. I sistemi di IA ad alto rischio sulla occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo	241
4. Riflessioni finali	243
<i>Riferimenti bibliografici</i>	244
CAPITOLO XV	
I SISTEMI DI IA AD ALTO RISCHIO IN AMBITO SANITARIO	
Commento all'Allegato III, par. 5	
<i>Paolo Gambatesa</i>	246
1. Introduzione: l'Allegato III, punto 5, dell' <i>AI Act</i> come snodo tra regolazione tecnologica e garanzia del diritto alla salute	246
2. Valutazione dell'ammissibilità alle prestazioni sanitarie pubbliche	248
3. Assicurazioni sanitarie e valutazione algoritmica del rischio	250
4. Emergenze sanitarie, triage e definizione delle priorità	253
5. Notazioni conclusive sul diritto alla salute alla prova dell'IA	255
<i>Riferimenti bibliografici</i>	256

pag.

CAPITOLO XVI

I SISTEMI AD ALTO RISCHIO IN MATERIA
DI IMMIGRAZIONE

Commento all'Allegato III, par. 7

Cecilia Siccardi

258

1. Premessa 258
 2. Il contesto: la *governance* digitale dell'immigrazione e degli *smart borders* 259
 3. La qualificazione come sistemi ad alto rischio: una scelta opportuna 263
 4. La disciplina dei sistemi ad alto rischio per il controllo dell'immigrazione: garanzie ed eccezioni 266
 5. Alcuni possibili vuoti di tutela? 269
 6. I sistemi vietati 271
 7. Riflessioni conclusive 272
- Riferimenti bibliografici* 273

CAPITOLO XVII

I SISTEMI AD ALTO RISCHIO IN MATERIA DI GIUSTIZIA

Commento all'Allegato III, par. 8

Elisa Pignanelli

275

1. La funzione del par. 8 dell'Allegato III e la qualificazione *ex ante* dei sistemi di IA in ambito giurisdizionale 275
 2. Ambito soggettivo e oggettivo della lett. a): l'assistenza algoritmica al giudice tra supporto e condizionamento 277
 3. Sistemi di intelligenza artificiale, giusto processo e diritto di difesa: trasparenza, intelligibilità e controllo umano della decisione giudiziaria 279
 4. Uguaglianza, non discriminazione e rischio di cristallizzazione della decisione giudiziale 282
 5. Riflessioni conclusive: la funzione giurisdizionale tra innovazione tecnologica e limiti costituzionali 284
- Riferimenti bibliografici* 287

B) *Requisiti*

CAPITOLO XVIII

IL SISTEMA DI GESTIONE DEL RISCHIO NEI SISTEMI
DI IA AD ALTO RISCHIO

Commento all'art. 9

Paolo Gambatesa

288

1. Il sistema di gestione del rischio come architrave dell'approccio europeo all'IA 288
2. Contenuto e struttura del sistema di gestione del rischio lungo il ciclo di vita di un sistema di IA 290
3. Responsabilità del provider e integrazione tra misure tecniche e organizzative 292
4. Documentazione, tracciabilità e funzione sistemica dell'art. 9 294
5. La gestione del rischio e il suo riflesso sulla tutela dei diritti fondamentali. Alcuni spunti conclusivi 296

Riferimenti bibliografici

297

CAPITOLO XIX

DATI E *GOVERNANCE* DEI DATI

Commento all'art. 10

Gregorio Cámara Villar

299

1. Introduzione contestuale: un diritto fondamentale al centro della società algoritmica 299
2. Senso e portata generale dell'art. 10 del Regolamento sull'Intelligenza Artificiale 300
3. I punti di forza normativi più significativi dell'art. 10 302
4. Quadro giurisprudenziale europeo applicabile all'art. 10: Corte di giustizia UE e CEDU 303
5. Alcuni punti critici degni di nota 304
 - 5.1. Assenza di definizione del soggetto interessato e ambiguità nella catena di responsabilità 304
 - 5.2. Visione parziale del ciclo di vita dei dati e omissione del regime delle licenze 305
 - 5.3. Dall'obbligo di risultato allo standard flessibile: una certa diluizione normativa dell'art. 10 305
 - 5.4. Il paradosso della qualità senza criteri: dipendenza dalla standardizzazione tecnica 306

	<i>pag.</i>
5.5. Autocertificazione e deficit di garanzie: il problema della valutazione di conformità	306
5.6. Ambiguità relativa sulla base giuridica per l'uso dei dati personali	307
5.7. Inadeguatezza del termine «rappresentatività» (art. 10, par. 3)	307
5.8. Mancata integrazione della valutazione d'impatto nel design tecnico (art. 10)	307
5.9. Lacune riguardo ai sistemi privi di addestramento	308
5.10. Rischi emergenti non espressamente contemplati nell'art. 10	309
6. Applicazione pratica e sfide di implementazione	309
7. Conclusione	311
<i>Riferimenti bibliografici</i>	311

CAPITOLO XX

PRINCIPI GENERALI DELL'IA: TRASPARENZA
E COMUNICAZIONE

Commento agli artt. 11-13 e 50

Eloísa Pérez Conchillo

1. Introduzione	313
2. Art. 11 AI Act: documentazione tecnica	315
3. Art. 12 AI Act: conservazione dei registri	317
4. Art. 13 AI Act: trasparenza e comunicazione delle informazioni ai responsabili del dispiegamento	319
5. Art. 50 AI Act: obblighi di trasparenza dei fornitori e dei responsabili del dispiegamento di determinati sistemi di IA	321
6. Conclusioni	325
<i>Riferimenti bibliografici</i>	326

CAPITOLO XXI

PRINCIPI GENERALI DELL'IA: LA SORVEGLIANZA
UMANA. SCELTA DI PRINCIPIO E SUE RICADUTE
PRATICHE

Commento all'art. 14

Irene Pellizzone

1. Breve panoramica introduttiva sulla struttura dell'art. 14: una norma ambiziosa ma inevitabilmente generica	328
2. Al di là della presunzione della superiorità del controllo umano: la scelta antropocentrica alla base della sorveglianza umana	330

	<i>pag.</i>
3. I corollari della introduzione di una sorveglianza umana obbligatoria nei sistemi di IA ad alto rischio: trasparenza, spiegabilità e responsabilità	331
4. Lo scetticismo intorno alla concreta attuazione della sorveglianza umana	333
5. La sorveglianza umana sotto le lenti del diritto costituzionale: alcuni spunti interpretativi in tema di <i>governance</i> e natura procedurale della garanzia	336
6. Esiste un diritto alla sorveglianza umana?	338
7. Osservazioni conclusive sulla corretta interpretazione della supervisione umana: il faro del principio personalista	339
<i>Riferimenti bibliografici</i>	340

CAPITOLO XXII

PRINCIPI GENERALI DELL'AI: ACCURATEZZA, ROBUSTEZZA E CIBERSICUREZZA

Commento all'art. 15

<i>Niccolò Panigada</i>	342
1. L'art. 15 nel contesto del sistema di requisiti per i sistemi di IA ad alto rischio	342
2. Le definizioni	343
2.1. Il concetto di accuratezza: tra performance tecnica, affidabilità decisionale e tutela dei diritti fondamentali	343
2.2. La robustezza dei sistemi di IA: resilienza tecnica e prevenzione dell'errore sistemico	345
2.3. La cibernsicurezza come requisito giuridico: protezione contro attacchi, manipolazioni e interferenze esterne	347
3. L'interrelazione tra accuratezza, robustezza e cibernsicurezza e il loro ruolo nella prevenzione di violazione dei diritti	349
<i>Riferimenti bibliografici</i>	351

C) *Obblighi dei fornitori*

CAPITOLO XXIII

OBBLIGHI E RESPONSABILITÀ NELLA CORNICE NORMATIVA DELL'AI ACT

Commento agli artt. 16-26

<i>Pietro Villaschi</i>	352
1. Gli artt. 16-26 come "cuore operativo" dell'AI ACT	352
2. Gli obblighi essenziali dei <i>provider</i>	353
3. Gli obblighi essenziali dei <i>deployer</i>	354
4. Una responsabilità lungo tutta la catena del valore	355

	<i>pag.</i>
5. I profili di responsabilità	356
6. Notazioni conclusive	359
<i>Riferimenti bibliografici</i>	360

CAPITOLO XXIV

LA VALUTAZIONE D'IMPATTO SUI DIRITTI
FONDAMENTALI PER I SISTEMI DI IA AD ALTO RISCHIO
Commento all'art. 27

<i>Marilisa D'Amico, Paolo Gambatesa</i>	361
1. Il c.d. <i>risk approach</i> applicato anche alla tutela dei diritti fondamentali. Notazioni introduttive sulla valutazione di impatto	361
2. La valutazione di impatto <i>ex art. 27</i> : metodo, contenuti e procedure	363
2.1. I soggetti obbligati, l'oggetto e i contenuti minimi (art. 27, par. 1).	363
2.2. La tempistica, l'aggiornamento e il "riuso" delle valutazioni (art. 27, par. 2)	367
2.3. La procedura di notifica all'autorità di vigilanza (art. 27, par. 3)	367
2.4. Il coordinamento con la valutazione di impatto prevista dal GDPR (art. 27, par. 4)	368
2.5. Il modello di questionario e il supporto dell'Ufficio per l'IA (art. 27, par. 5)	369
3. Potenzialità e criticità della valutazione di impatto sui diritti fondamentali	369
4. Alla ricerca di necessari compromessi tra il linguaggio dei diritti fondamentali e il linguaggio informatico: alcuni spunti conclusivi	373
<i>Riferimenti bibliografici</i>	374

SEZIONE IV

ORGANIZZAZIONE DEL POTERE E STRUMENTI
DI RACCORDO TRA UE E STATI MEMBRI

CAPITOLO XXV

IL SISTEMA DI *GOVERNANCE* A LIVELLO EUROPEO
E NAZIONALE

Commento agli artt. 64-70

<i>Stefano Catalano, Stefania Leone</i>	379
1. La necessità di una <i>governance</i> articolata e integrata, sia per dare applicazione al Regolamento, sia per "stare al passo"	379

	<i>pag.</i>
2. L'ufficio per l'IA	381
3. Il Comitato per l'IA europeo per l'intelligenza artificiale	383
4. Il Forum consultivo	385
5. Il Gruppo di esperti scientifici	386
6. Le autorità nazionali	388
7. Conclusioni	389
<i>Riferimenti bibliografici</i>	391

CAPITOLO XXVI

LA PROCEDURA DI NOTIFICA

Commento agli artt. 28-39

<i>Amalia Lozano España</i>	392
1. Introduzione	392
2. Soggetti e presupposti del procedimento di notifica	393
2.1. I soggetti coinvolti	393
2.2. I presupposti procedurali	397
3. Il procedimento di notifica	399
4. Ipotesi di inadempimento da parte di un organismo notificato	401
5. Conclusione	402
<i>Riferimenti bibliografici</i>	402

CAPITOLO XXVII

ATTI DELLA COMMISSIONE E *GOVERNANCE* NEL
REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE

<i>Miguel José Arjona Sánchez</i>	403
1. Introduzione	403
2. La via normativa della Commissione	405
2.1. Atti delegati: fondamento, portata e limiti	406
2.2. Atti di esecuzione (normazione, specificazioni comuni e armonizzazione dei <i>sandboxes</i>)	408
3. La via organica o della <i>governance</i>	412
3.1. La Commissione nel governo multilivello dell'AI Act	413
3.2. L'architettura istituzionale al servizio della Commissione	414
3.2.1. L'Ufficio per l'Intelligenza Artificiale	414
3.2.2. Il Comitato Europeo per l'Intelligenza Artificiale	414
3.2.3. Il foro consultivo e il gruppo di esperti scientifici indipendenti	414

	<i>pag.</i>
4. Funzioni di supervisione e compliance (in chiave multilivello)	415
4.1. Supervisione selettiva dei GPAI e “dialogo strutturato”	416
4.2. Coordinamento con le autorità nazionali di vigilanza del mercato	417
4.3. Organismi notificati: requisiti e controllo coordinato	417
4.4. Sfide e tensioni nella <i>governance</i> della Commissione	418
<i>Riferimenti bibliografici</i>	418

CAPITOLO XXVIII

IL RICORSO ALLE NORME ARMONIZZATE NELLA
REGOLAMENTAZIONE EUROPEA DELL’INTELLIGENZA
ARTIFICIALE: CRITICITÀ E PROSPETTIVE

Commento agli artt. 40-49

Giacomo Palombino

420

1. Premessa	420
2. Il ricorso a <i>norme armonizzate</i> nell’ordinamento europeo	421
3. Il ricorso a <i>norme armonizzate</i> nella regolamentazione dell’intelligenza artificiale	423
4. Riflessioni conclusive: alla ricerca di un equilibrio tra esigenze (non necessariamente) contrapposte	425
<i>Riferimenti bibliografici</i>	427

SEZIONE V

MODELLI DI IA PER FINALITÀ GENERALI

CAPITOLO XXIX

I MODELLI DI INTELLIGENZA ARTIFICIALE PER
FINALITÀ GENERALE. INQUADRAMENTO,
DISCIPLINA E BUONE PRASSI

Commento agli artt. 51-56

Marta Annamaria Tamborini

431

1. Introduzione: la collocazione dell’intelligenza artificiale generativa nel Regolamento europeo sull’Intelligenza artificiale	431
2. Definizione dei modelli a finalità generale, distinzione rispetto ai sistemi di intelligenza artificiale (preambolo e art. 3)	434
3. Distinzione e classificazione tra modelli a finalità generale e sistemi a finalità generale che presentano rischio sistemico	436

	<i>pag.</i>
4. La regolamentazione prevista dal quadro europeo, il ruolo delle buone prassi	439
5. Questioni aperte alla luce della proposta di revisione della materia attraverso il c.d. "Digital Omnibus"	441
6. Considerazioni conclusive	442
<i>Riferimenti bibliografici</i>	443

SEZIONE VI SORVEGLIANZA, CONTROLLO E SANZIONI

CAPITOLO XXX

MONITORAGGIO, APPLICAZIONE E GARANZIE, SANZIONI

Commento agli artt. 72-94 e 99-101

<i>Rosa Iannaccone</i>	447
1. Un quadro d'insieme: dal monitoraggio al regime sanzionatorio	447
2. Monitoraggio, vigilanza e supervisione dei sistemi di intelligenza artificiale	448
3. Il regime sanzionatorio e le garanzie procedurali nel sistema europeo di regolazione dell'intelligenza artificiale	453
<i>Riferimenti bibliografici</i>	456

CAPITOLO XXXI

IL RUOLO DELLA *SOFT LAW* NELL'ATTUAZIONE DELL'AI ACT

Commento agli artt. 95 e 96

<i>Pietro Villaschi</i>	457
1. Premessa	457
2. L'art. 95 dell'AI ACT e i Codici di condotta	459
2.1. I codici di condotta definiti dall'AI ACT: natura, opportunità e rischi	460
3. Le linee guida <i>ex art.</i> 96 e l'attuazione uniforme dell'AI ACT in tutto il territorio dell'Unione europea	462
4. L'interazione fra gli artt. 95 e 96 dell'AI ACT: il ruolo della <i>soft law</i> nella regolazione dell'intelligenza artificiale	464
<i>Riferimenti bibliografici</i>	465

PARTE II

LA LEGGE 23 SETTEMBRE 2025, N. 132

CAPITOLO I

PRINCIPI E FINALITÀ DELLA LEGGE ITALIANA

Commento all'art. 1

<i>Camilla Burelli</i>	469
1. Premessa	469
2. L'art. 1, comma 1: il perimetro applicativo della legge n. 132/2025	473
3. L'art. 1, comma 2: la norma di raccordo tra la disciplina nazionale e quella unionale	476
<i>Riferimenti bibliografici</i>	477

CAPITOLO II

LE DEFINIZIONI NELLA LEGGE ITALIANA

Commento all'art. 2

<i>Camilla Burelli</i>	479
1. Premessa	479
2. L'art. 2, comma 1: l'ambiguità della nozione di «modelli di IA» e la definizione autonoma di «dato»	479
3. L'art. 2, comma 2: il rinvio residuale all' <i>AI Act</i> (Regolamento UE 2024/1689)	483
<i>Riferimenti bibliografici</i>	484

CAPITOLO III

I PRINCIPI GENERALI DELLA LEGGE ITALIANA SULL'IA

Commento all'art. 3

<i>Ilaria Anrò</i>	485
1. I principi contemplati dalla norma, tra etica e diritto	485
2. Il principio antropocentrico	489
3. Il rispetto della vita politica ed istituzionale e la tutela del dibattito democratico	491
4. La legge italiana e il Regolamento (UE) 2024/1689	491
5. La cybersicurezza	493

	<i>pag.</i>
6. La tutela delle persone con disabilità	493
<i>Riferimenti bibliografici</i>	494
CAPITOLO IV	
I PRINCIPI IN MATERIA DI INFORMAZIONE E DI RISERVATEZZA DEI DATI PERSONALI	
Commento all'art. 4	
<i>Benedetta Liberali</i>	495
1. La collocazione della disposizione dedicata all'informazione, alla riservatezza dei dati e alla tutela dei minori in relazione all'intelligenza artificiale	495
2. Sulla garanzia della libertà di espressione e di informazione	497
3. Sulla garanzia della «riservatezza» (o meglio protezione) dei dati personali	500
4. Sull'accesso alle tecnologie di intelligenza artificiale da parte di minori e sul relativo trattamento dei dati personali	506
<i>Riferimenti bibliografici</i>	507
CAPITOLO V	
I PRINCIPI IN MATERIA DI SVILUPPO ECONOMICO ALLA PROVA DELL'IA	
Commento all'art. 5	
<i>Fabiola Giotto</i>	508
1. Introduzione	508
2. Lett. a): promozione dell'AI, competitività economica e antropocentrismo	510
3. Lett. b): verso la creazione di un mercato digitale competitivo ed equo	513
4. Lett. c): il dato come "risorsa strategica" per competitività e innovazione	514
5. Lett. d): la localizzazione dei dati strategici nelle scelte pubbliche di IA	517
6. Lett. e): dalla ricerca al mercato, l'IA come strumento per lo sviluppo eco- nomico	519
7. Conclusioni	520
<i>Riferimenti bibliografici</i>	522

pag.

CAPITOLO VI

LA SICUREZZA E LA DIFESA NAZIONALE NELLA LEGGE ITALIANA SULL'INTELLIGENZA ARTIFICIALE

Commento agli artt. 6 e 21

Elisa Pignanelli

523

1. Sicurezza nazionale, difesa nazionale e limiti costituzionali nell'uso dell'intelligenza artificiale: il perimetro dell'art. 6, comma 1, della legge n. 132/2025 523
 2. Norme speciali e garanzie residue nel trattamento dei dati per finalità di sicurezza: il modello dell'art. 6, comma 2, della legge n. 132/2025 527
 3. Il rinvio alla fonte regolamentare di cui all'art. 6, comma 3: una disciplina tecnica ad alta opacità 530
 4. L'art. 21 e la sperimentazione dell'intelligenza artificiale nei servizi del Ministero degli affari esteri e della cooperazione internazionale 532
 5. Riflessioni conclusive 534
- Riferimenti bibliografici* 535

CAPITOLO VII

I DIRITTI DELLE PERSONE CON DISABILITÀ DI FRONTE AI SISTEMI DI IA

Commento all'art. 7

Giuseppe Arconzo, Gaia Patarini

536

1. L'intelligenza artificiale al cospetto della disabilità: barriera o facilitatore? 536
 2. La strada seguita dal legislatore italiano 541
 3. Alcune considerazioni critiche: una legge a costo zero? 547
 4. Conclusioni 548
- Riferimenti bibliografici* 549

CAPITOLO VIII

L'USO DELL'INTELLIGENZA ARTIFICIALE IN AMBITO SANITARIO

Commento agli artt. 7, 8 e 10

Paolo Gambatesa

552

1. Introduzione. Dall'*AI Act* alla legge italiana sull'IA in materia sanitaria 552
2. L'art. 7 e le garanzie del diritto alla salute nell'uso dell'intelligenza artificiale 554
3. L'art. 8 tra ricerca scientifica, dati sanitari e sviluppo dell'IA 556

	<i>pag.</i>
4. L'art. 10 e il fascicolo sanitario elettronico come infrastruttura pubblica della sanità digitale	559
5. Dalla ricerca alla cura: l'intelligenza artificiale come sfida regolatoria per il diritto alla salute. Alcune considerazioni conclusive	562
<i>Riferimenti bibliografici</i>	563
CAPITOLO IX	
INTELLIGENZA ARTIFICIALE E DIRITTO DEL LAVORO	
Commento agli artt. 11-13	
<i>Alessandra Ingraio, Francesca Marinelli</i>	565
1. IA e diritto del lavoro: come si inserisce la legge n. 132/2025 nel diritto del lavoro vigente tra criticità e opportunità	565
2. L'art. 11: disposizioni sull'uso dell'IA in materia di lavoro	566
3. L'art. 12: l'Osservatorio sull'adozione di sistemi di IA nel mondo del lavoro	571
4. L'art. 13: disposizioni in materia di professioni intellettuali	572
<i>Riferimenti bibliografici</i>	573
CAPITOLO X	
L'USO DELL'INTELLIGENZA ARTIFICIALE NELLA PUBBLICA AMMINISTRAZIONE	
Commento all'art. 14	
<i>Lorenzo Grossi</i>	575
1. Introduzione	575
2. Art. 14, comma 1: i fini e i modi di utilizzo dei sistemi di intelligenza artificiale	576
3. Art. 14, comma 2: la garanzia dello <i>human in the loop</i>	581
4. Art. 14, commi 3 e 4: l'adeguamento dell'apparato amministrativo a risorse invariate	584
5. Conclusioni	587
<i>Riferimenti bibliografici</i>	588

pag.

CAPITOLO XI

L'IMPIEGO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE
NELL'ATTIVITÀ GIUDIZIARIA

Commento all'art. 15

<i>Marilisa D'Amico, Michael Bianchi</i>	590
1. Premessa: l'intelligenza artificiale e la giustizia tra innovazione e garanzie	590
2. L'utilizzo dell'IA da parte dei magistrati nello svolgimento dell'attività giurisdizionale	592
3. Le competenze del Ministero della Giustizia per l'impiego dell'IA nell'organizzazione dei lavori e nella formazione dei magistrati	595
4. Quale ruolo per l'avvocatura nel "silenzio" della legge?	598
5. Considerazioni conclusive	601
<i>Riferimenti bibliografici</i>	602

CAPITOLO XII

LA STRATEGIA NAZIONALE PER L'IA

Commento all'art. 19

<i>Nannerel Fiano</i>	603
1. Una <i>governance</i> istituzionale composita	603
2. Una strategia "sinergica"	605
3. Il Comitato di coordinamento	606
4. La Strategia italiana per l'intelligenza artificiale (2024-2026)	607
<i>Riferimenti bibliografici</i>	609

CAPITOLO XIII

LE AUTORITÀ NAZIONALI PER L'IA TRA VIGILANZA,
COORDINAMENTO E SVILUPPO

Commento all'art. 20

<i>Sara Di Giovanni</i>	610
1. L'ambito di applicazione e la <i>ratio</i> dell'art. 20	610
2. Il sistema delle Autorità nazionali designate: natura, funzioni e riparto di competenze	612
3. Il coordinamento istituzionale: il Comitato presso la Presidenza del Consiglio	615
4. Rapporti con AGCOM e Garante Privacy	616
5. Riflessioni conclusive	616
<i>Riferimenti bibliografici</i>	618

CAPITOLO XIV

L'IA COME CAMPO DI RICERCA E STRUMENTO
DI INCLUSIONE: MISURE DI SOSTEGNO AI GIOVANI
E ALLO SPORT

Commento all'art. 22

Michael Bianchi

619

1. Quale ruolo per i diritti costituzionali di fronte all'impiego dell'IA nei campi dell'istruzione e dello sport? 619
 2. Misure di sostegno ai giovani che vogliono studiare l'IA o abbiano fatto ricerca su di essa 621
 3. Misure di sostegno allo sport: l'IA come strumento di inclusione nel fenomeno sportivo 624
 4. Riflessioni conclusive 627
- Riferimenti bibliografici* 628

CAPITOLO XV

CYBERSICUREZZA E SOVRANITÀ TECNOLOGICA
NELLA LEGGE ITALIANA

Commento agli artt. 18 e 23

Marta Annamaria Tamborini

630

1. Introduzione: la collocazione dell'intelligenza artificiale generativa nel Regolamento europeo sull'Intelligenza artificiale 630
 2. Il contesto europeo in materia di cybersicurezza, fra sicurezza, diritti fondamentali e affidabilità dei sistemi di intelligenza artificiale 631
 3. L'art. 18 e la valorizzazione dell'IA per la sicurezza cibernetica e cooperazione pubblico-privato 633
 4. L'art. 23 e la previsione di investimenti pubblici in IA e cybersicurezza 635
 5. Garanzie, controlli e possibili criticità applicative 636
 6. Conclusioni 637
- Riferimenti bibliografici* 638

CAPITOLO XVI

L'ADEGUAMENTO DELL'ORDINAMENTO NAZIONALE
ALL'AI ACT TRA LEGGE E DELEGA LEGISLATIVA

Commento agli artt. 16 e 24

Costanza Nardocci

639

1. Una premessa di fondo o di metodo: la prima "legge", ma ... il Governo 639

	<i>pag.</i>
2. La “buona” delega? L’art. 16 e la disciplina (governativa, ma tecnica) di dati, algoritmi e metodi matematici per l’addestramento dei sistemi di IA	641
2.1. La flessibilizzazione (interna) dell’“alto rischio”: ma non dovevano occuparsene la Commissione e il Parlamento UE?	646
3. L’art. 24 e la delega ampia (<i>rectius</i> , le due deleghe)	648
3.1. I commi 1 e 2: la prima delega e l’adeguamento interno all’ <i>AI Act</i> tra prerogative delle autorità nazionali per l’intelligenza artificiale, formazione e ricerca	650
3.1.1. Ancora sulle autorità interne: il mancato seguito degli art. 78, comma 4, e art. 77 <i>AI Act</i> ?	652
3.1.2. Un settore delicato e trascurato: l’utilizzo dei sistemi di intelligenza artificiale da parte delle forze di polizia e il mancato art. 24- <i>bis</i>	654
3.2. La seconda delega e il comma 3: di materia penale, intelligenza artificiale, riserva di legge e rischi di responsabilità oggettiva	658
4. Considerazioni conclusive tra <i>tempi</i> del Governo e <i>tempi</i> dell’Unione Europea	663
<i>Riferimenti bibliografici</i>	665

CAPITOLO XVII

IL DIRITTO D’AUTORE DAVANTI ALLA “CREATIVITÀ”
DELL’INTELLIGENZA ARTIFICIALE

Commento all’art. 25

<i>Niccolò Panigada</i>	667
1. Premessa	667
2. Il nuovo art. 1 della legge italiana sul diritto d’autore	669
3. La nuova regolamentazione per l’uso di opere protette tra <i>Text and Data Mining</i> e Intelligenza artificiale	669
4. Alcuni casi esaminati dalla giurisprudenza di opere generate dall’IA	671
<i>Riferimenti bibliografici</i>	675

CAPITOLO XVIII

LE DISPOSIZIONI PENALI: L’IA COME *INSTRUMENTUM*
SCELERIS

Commento all’art. 26

<i>Beatrice Fragasso</i>	676
1. Intelligenza artificiale e responsabilità penale: una premessa	676

	<i>pag.</i>
2. La definizione di intelligenza artificiale come elemento normativo delle disposizioni penali (rinvio)	678
3. La fattispecie di illecita diffusione di contenuti generati o manipolati artificialmente	680
4. La nuova fattispecie in materia di diritto d'autore	684
5. Le nuove circostanze aggravanti	685
6. Brevi cenni ai criteri di delega in materia penale contenuti nell'art. 24 e conclusioni	687
<i>Riferimenti bibliografici</i>	689

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 Constitucional, 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 SCCELERIS*
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 penale¹.

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 supervisionarlo². 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. GIANINI, *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 europea³, 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 tempo⁴.

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 sfuggenti⁵. 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 subite dalla norma definitoria nel corso del processo di approvazione del Regolamento, v. diffusamente C. TRINCADO CASTAN, *The legal concept of artificial intelligence: the debate surrounding the definition of AI System in the AI Act*, in *BioLaw Journal-Riv. BioDiritto*, 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

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

danno ingiusto non debba necessariamente avere un contenuto patrimoniale⁷. 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 sessuale⁹.

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 privacy e riservatezza*, Giappichelli, Torino, 2024, p. 157 ss.

¹⁰ A. GULLO, R. FLOR, *Italian report on criminalisation of AI-related offences*, in F. MIRÓLLINARES, 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 domestica¹², che richiede agli Stati membri che venga incriminata la seguente condotta intenzionale: «produrre, manipolare o alterare e successivamente rendere accessibile al pubblico, tramite TIC¹³, 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 ucraino¹⁵.

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 democratiche¹⁷. 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 offensività¹⁹.

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*, ovvero sia 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 scientifici²⁰ e di contributi pubblicati sui siti dei quotidiani²¹.

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.), aggrottaggio (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 incriminatrici²⁶: 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 aggravanti²⁷.

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 umano²⁸.

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 infau-
sti*, 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 responsabi-
lità 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-crimi-
nali e interpretazione della nozione di violenza nel diritto penale delle tecnologie digi-
tali*, 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.), *Criminalisa-
tion 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: Crisis 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.