

INDICE

Prefazione - Paolo Benanti	pag.	11
Prefazione - Giulio Bacosi	pag.	13
Introduzione	pag.	16
L'evoluzione degli illeciti nell'era dell'IA	pag.	20
1. Introduzione	»	20
2. Cybercrime avanzato e automazione delle violazioni	»	23
3. Utilizzo illecito delle criptovalute	»	26
4. Manipolazione algoritmica dei mercati finanziari	»	30
5. Furto dei dati e violazioni sistemiche	»	35
6. Frodi d'identità e deepfake economy	»	38
7. Approfondimento: superficie di attacco e punti deboli	»	41
8. IA tra minaccia e presidio: verso una governance integrata.....	»	46
Profili giuridici e investigativi dell'IA	pag.	48
1. Premessa: l'evoluzione della responsabilità penale nell'era dell'IA.....	»	48
2. Una nozione penalisticamente orientata di intelligenza artificiale	»	49
3. Le principali problematiche giuridiche	»	51
3.1. Dalla personalità della responsabilità penale all'autonomia della macchina	»	51
3.2. Tentativi di delineare una responsabilità diretta dell'IA	»	53
3.3. La responsabilità delle persone fisiche "dietro la macchina"	»	55
4. La tassonomia delle fattispecie penalmente rilevanti.....	»	66
4.1. Reati colposi e intelligenza artificiale	»	66
4.2. Reati dolosi e nuove opportunità criminose.....	»	68
4.3. Il "reato algoritmico": verso una categoria ibrida	»	70
5. I profili di responsabilità dell'ente.....	»	72
5.1. Il catalogo dei reati-presupposto e la sfida della delega legislativa...	»	73
5.2. Dalla colpa individuale alla colpa organizzativa: il cambio di prospettiva	»	74

5.3. L'applicazione del modello del D.Lgs. n. 231/2001: struttura e elementi	»	75
5.4. Approfondimento: case study	»	78
6. Sanzionabilità in via amministrativa per il mancato rispetto di norme cautelative di settore - rapporto con la responsabilità amministrativa degli enti	»	81
7. Intelligenza artificiale e responsabilità civile da prodotto intelligente difettoso	»	82
8. Profili investigativi	»	88
8.1. La prova digitale: acquisizione e conservazione, validità processuale, sfide tecniche e giuridiche	»	89
8.2. Incidenti probatori e digital forensics: un rapporto necessario....	»	92
8.3. Il valore probatorio delle comunicazioni digitali	»	99
8.4. Perquisizioni digitali e ausiliario di P.G.	»	104
8.5. Il sequestro di materiale informatico: procedure operative, aspetti tecnici, giurisprudenza rilevante	»	107
8.6. Tecniche di sequestro di criptovalute	»	109
8.7. Collaborazione con gli exchange e tracciamento dei flussi illeciti..	»	111
8.8. Le sfide investigative nel dark web	»	113

Principali disposizioni normative e regolamentari in materia di IA pag. 115

1. AI Act: Regolamento (UE) 2024/1689 del 13 giugno 2024	»	115
1.1. Inquadramento generale: dalla neutralità tecnologica al governo del rischio	»	115
1.2. Pratiche vietate: il criterio dell'inaccettabilità	»	117
1.3. Sistemi ad alto rischio: dalla qualificazione al presidio.....	»	123
1.4. Requisiti obbligatori per i sistemi ad alto rischio: dalla norma all'architettura tecnica e organizzativa	»	127
1.5. Monitoraggio post-market, incident management e doveri di reazione lungo il ciclo di vita	»	134
1.6. Modelli di IA di uso generale (General Purpose AI Models): obblighi specifici e responsabilità nella catena di fornitura	»	134
1.7. Conformità, verificabilità e governance dell'enforcement	»	136
1.8. Tempistica di applicazione e progressiva operatività dell'AI Act	»	139
2. Sicurezza e resilienza dell'ecosistema digitale	»	141
2.1. La Direttiva NIS2	»	141
2.2. Il Cyber Resilience Act (CRA)	»	145
2.3. Il Digital Operational Resilience Act (DORA).....	»	149
3. La governance degli ecosistemi digitali	»	153
3.1. Il Digital Services Act (DSA)	»	153

3.2.	Il Digital Markets Act (DMA)	»	158
3.3.	Il Digital Omnibus	»	161
4.	Protezione dei dati personali e garanzie fondamentali: GDPR e discipline complementari	»	164
4.1.	Il GDPR come statuto generale del trattamento nell'ecosistema dell'IA	»	165
4.2.	Dati personali, dati sensibili e limiti all'espansione funzionale dell'IA	»	166
4.3.	Decisioni automatizzate, valutazioni d'impatto e tutela dei diritti fondamentali	»	166
4.4.	Discipline complementari e funzione sistemica delle autorità di garanzia	»	167
5.	Accesso ai dati, prova elettronica e cooperazione investigativa: il Regolamento e-Evidence	»	168
5.1.	Oggetto, finalità e strumenti del Regolamento	»	169
5.2.	Categorie di dati, soglie di accesso e proporzionalità investigativa	»	170
5.3.	Diritti fondamentali, protezione dei dati e garanzie procedurali	»	171
5.4.	Cooperazione investigativa, soggetti privati e nuovi equilibri istituzionali	»	173
6.	La normativa nazionale tra cybersicurezza, intelligenza artificiale e coordinamento con la cornice europea	»	174
6.1.	La Legge n. 90 del 2024: rafforzamento della prevenzione e del coordinamento	»	175
6.2.	Il completamento del quadro: il recepimento della "NIS 2" e la Legge n. 132 del 2025 sull'intelligenza artificiale	»	180
6.3.	Coordinamento con la cornice europea già esaminata	»	185

Intelligenza artificiale e Pubblica Amministrazione: sfide, norme e prospettive pag. 187

1.	L'automazione dei procedimenti amministrativi e la decisione amministrativa algoritmica	»	187
1.1.	Governare l'algoritmo: norme europee e italiane sull'intelligenza artificiale nella Pubblica Amministrazione	»	194
1.2.	La decisione algoritmica	»	198
1.3.	Struttura della decisione amministrativa automatizzata e centralità del responsabile del procedimento	»	200

2. Sindacato del giudice amministrativo sulle decisioni AI-based	»	202
2.1. Decisione amministrativa automatizzata e funzione giurisdizionale: il giudice come garante dei diritti nell'era digitale	»	204
2.2. Il contributo della giurisprudenza del Consiglio di Stato: prime applicazioni e sviluppo del principio di legalità algoritmica	»	205
2.3. Riconfigurazione delle categorie giuridiche e sindacabilità delle decisioni algoritmiche: verso una "giurisdizione piena" in chiave sostanziale.....	»	211
3. Il fenomeno della shadow AI e i rischi di opacità.....	»	215
3.1. Shadow AI e diritto comparato: approcci internazionali alla regolazione dell'intelligenza artificiale non governata nella Pubblica Amministrazione	»	216
3.2. Profili di legalità e accountability: verso una responsabilità multilivello.....	»	218
3.3. Meccanismi di contrasto oltre l'audit. Verso un'architettura preventiva e adattiva	»	219
4. Strategia italiana per l'impiego dell'intelligenza artificiale nella Pubblica Amministrazione.....	»	222
4.1. L'Italia e l'Intelligenza Artificiale: tra eccellenza accademica e ritardi applicativi	»	225
4.2. Settori prioritari e ambiti di applicazione dell'intelligenza artificiale.....	»	229
4.3. Le azioni strategiche nella Pubblica Amministrazione: tra obiettivi e gestione dei rischi	»	230

Prevenzione e gestione dei rischi per gli illeciti inerenti a sistemi di intelligenza artificiale

1. Prevenzione e gestione dei rischi nel settore pubblico	»	234
1.1. Il ruolo dei Piani Triennali di Prevenzione della Corruzione e della Trasparenza (PTPCT)	»	236
1.2. Utilizzo dell'Intelligenza Artificiale per la prevenzione della corruzione e il controllo delle decisioni algoritmiche.....	»	239
1.3. Gestione delle segnalazioni di illeciti nell'uso dell'IA (whistleblowing, audit, accountability).....	»	241
1.4. Opportunità: trasparenza, efficienza, automazione dei controlli	»	243
1.5. Sfide: responsabilità disciplinare, tutela dei dati, resistenza al cambiamento	»	244
2. Intelligenza artificiale, diritto penale e responsabilità	»	247
2.1. Profili di responsabilità penale dell'intelligenza artificiale nel settore privato.....	»	247

2.2. Reati informatici, Modelli 231, intelligenza artificiale e supply chain..... »	248
2.3. La gestione del rischio informatico nel Modello 231, mappatura dei processi, protocolli aziendali e codice etico »	251
2.4. Opportunità offerte dall'IA per la sicurezza aziendale (monitoraggio e anomaly detection) »	254
2.5. Modelli organizzativi integrati: privacy e integrazione delle funzioni »	255
2.6. Impatto dell'intelligenza artificiale sull'Organismo di Vigilanza: incombenze ed opportunità..... »	257
2.7. Formazione e comunicazione interna..... »	262
2.8. Possibili accortezze di prevenzione dagli attacchi hacker »	264
2.9. Sfide: gestione del rischio e cultura della sicurezza »	267
2.10. Sicurezza informatica e PMI »	268

Opportunità offerte dall'IA in attività di law enforcement e di controllo in materia fiscale..... pag.	273
1. Premessa..... »	273
2. Sviluppo dell'intelligenza artificiale nel contesto delle forze dell'ordine ... »	275
2.1. Un processo di evoluzione per fasi »	275
2.2. L'apporto dell'IA nelle attività di intelligence e nei centri di comando e controllo »	276
2.3. Limiti e problematiche »	277
3. Principali applicazioni di IA: sistemi di sorveglianza intelligente, riconoscimento facciale e biometrico, veicoli e droni autonomi..... »	278
3.1. Sorveglianza intelligente, analisi video automatizzata, riconoscimento facciale e identificazione biometrica..... »	278
3.2. Veicoli e droni autonomi per il controllo del territorio..... »	281
4. I sistemi di predictive policing: dalla reazione alla prevenzione, come cambia il paradigma operativo..... »	283
4.1. Origine e tipologie di sistemi di polizia predittiva »	285
4.2. I principali profili di criticità degli strumenti di predictive policing..... »	288
4.3. L'evoluzione dell'inquadramento normativo dei sistemi di polizia predittiva nell'AI Act..... »	291
4.4. Il quadro di governance e di enforcement costruito dall'AI Act.. »	294
4.5. Prospettive applicative dei sistemi di predictive policing nell'ordinamento nazionale..... »	296
4.6. Considerazioni conclusive..... »	298

5. L'intelligenza artificiale nell'analisi del rischio fiscale: modelli predittivi e metodologie integrate..... »	299
5.1. Una panoramica introduttiva su IA e Amministrazione finanziaria in Italia »	301
5.2. La strategia nazionale per l'IA e la trasformazione digitale della funzione fiscale..... »	303
5.3. Il ruolo strategico dell'IA nel risk management fiscale..... »	304
5.4. Dalla Legge Delega n. 111/2023 al D.Lgs. n. 13/2024..... »	306
5.5. Strumenti di intelligenza artificiale nell'attività dell'Agenzia delle Entrate..... »	311
5.6. Profili di tutela del contribuente sottoposto alle procedure automatizzate: alla ricerca dell'equilibrio tra diritti e lotta all'evasione »	317

Etica e IA: principi, sfide e prospettive per una governance responsabile pag. 330

1. Dilemmi etici e sociali nell'utilizzo dell'IA nelle attività di polizia e della Pubblica Amministrazione »	330
1.1. Bias algoritmici e discriminazione automatica »	332
1.2. Trasparenza e spiegabilità degli algoritmi..... »	338
1.3. Responsabilità, accountability e sistemi di controllo »	341
1.4. Erosione del controllo umano: il principio "human in the loop". »	343
1.5. Rischi di autoritarismo algoritmico e squilibri di potere informativo »	345
2. Impatto etico dell'Intelligenza Artificiale sulla società e l'ambito privacy »	347
2.1. Etica e intelligenza artificiale..... »	347
2.2. Privacy e sorveglianza di massa »	350
2.3. L'AI Act e la protezione dei dati personali..... »	353
2.4. IA e diritto alla privacy: un equilibrio in trasformazione tra GDPR, AI Act e Digital Omnibus..... »	356
2.5. Il concetto di inferenza nell'intelligenza artificiale e le implicazioni sulla privacy »	361
2.6. Trasparenza, consapevolezza e controllo dell'interessato sulle inferenze automatizzate »	363
2.7. Conseguenze pratiche: discriminazione, esclusione e profiling predittivo..... »	365
3. Sicurezza cibernetica e IA: rischi, vulnerabilità e dilemmi etici..... »	367
3.1. Tecniche di attacco..... »	369
3.2. Contromisure di sicurezza per mitigare i rischi legati all'AI..... »	373

3.3. Etica e responsabilità nell'adozione dell'intelligenza artificiale... »	374
4. Soluzioni proposte »	376
4.1. L'adozione di un approccio algoretico »	376
4.2. Il Codice etico AgID »	378
4.3. Le raccomandazioni ICSC (Centro Nazionale di Ricerca in HPC, Big Data e Quantum Computing) »	380
Conclusioni pag.	383
Normativa, regolamenti, linee guida pag.	387
Giurisprudenza pag.	390
Bibliografia pag.	391
Sitografia pag.	402