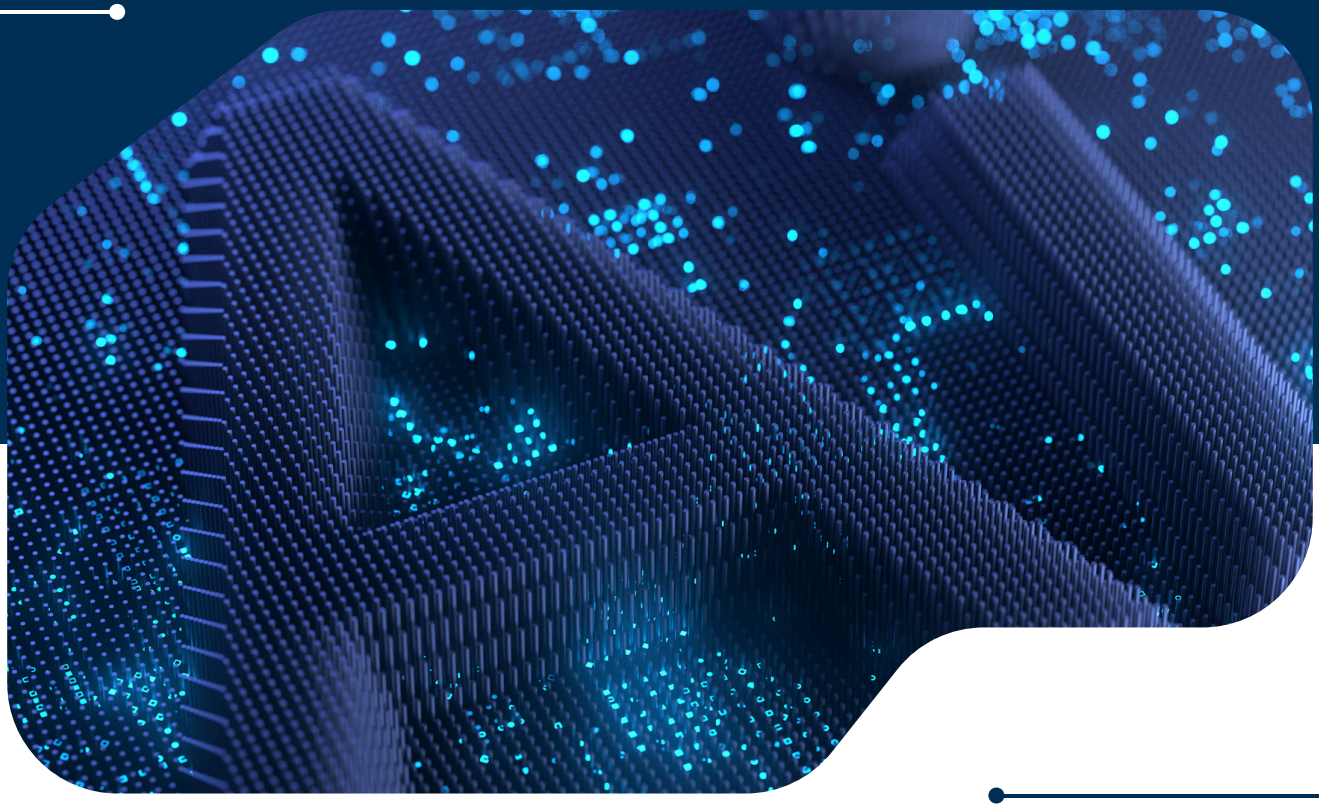

RESPONSABILITA' PENALE E INTELLIGENZA ARTIFICIALE: PROFILI GIURIDICI E QUESTIONI APERTE

Position Paper

GEBBIABORTOLOTTO
PENALISTI ASSOCIATI

Luglio 2025
www.gbpenalisti.it

SOMMARIO

INTRODUZIONE

Rilevanza del tema nell'attuale contesto giuridico

In conformità con una definizione ampiamente recepita in ambito internazionale, l'intelligenza artificiale si configura quale ramo specialistico dell'informatica, volto all'indagine dei presupposti teorici, delle metodologie algoritmiche e delle tecniche ingegneristiche che consentono la progettazione di sistemi di *hardware* e *software* capaci di compiere operazioni che, in apparenza, rientrerebbero nel dominio esclusivo delle facoltà cognitive umane.[1] Tali sistemi, mediante l'elaborazione autonoma di dati, l'apprendimento automatico e la progressiva raffinazione delle risposte, si rendono idonei a simulare dei comportamenti intelligentemente orientati a scopi determinati.[2]

L'evoluzione esponenziale delle tecnologie intelligenti, nonché la loro pervasiva diffusione nei più eterogenei ambiti dell'agire umano, impongono una riflessione profonda, critica e sistematica circa l'impatto che tali innovazioni producono sul piano della regolazione giuridica. In questa sede, l'analisi si concentra precipuamente sull'interazione tra intelligenza artificiale e diritto penale sostanziale, settore nel quale l'affermazione di agenti artificiali dotati di crescente autonomia operativa, ha determinato una frizione evidente con i modelli dogmatici tradizionali di imputazione soggettiva e responsabilità personale.

Tra le questioni maggiormente dibattute, oltre alla problematica relativa alla possibile configurabilità delle entità artificiali quali potenziali autori di reato, si collocano ulteriori interrogativi di rilievo sistemico, concernenti la riconducibilità della responsabilità penale a soggetti giuridici tradizionali, ovverosia persone fisiche e giuridiche che, a vario titolo, intervengono nella catena di ideazione, sviluppo, distribuzione ed impiego del sistema di intelligenza artificiale.

[1] M. Somalvico, *Intelligenza artificiale*, Milano, 1987.
[2] Vd. il report *ID R&D Human or Machine: AI Proves Best at Spotting Biometric Attacks*, 2022.

La difficoltà, in tal caso, consiste nell'individuare con precisione il segmento della filiera tecnologica ove si innesti una condotta penalmente rilevante, nonché nel determinare se tale condotta integri gli estremi di una fattispecie tipica, colpevole ed offensiva, secondo i canoni di tassatività, offensività e personalità della responsabilità penale.

A rendere ancora più complessa tale ricostruzione concorrono talune caratteristiche intrinseche dei sistemi di intelligenza artificiale, che pongono sfide inedite ai tradizionali schemi della causalità penalistica. In particolare, la catena causale nei malfunzionamenti derivanti da sistemi intelligenti risulta estremamente articolata, e l'individuazione del soggetto cui attribuire le responsabilità dell'evento lesivo implica la ricostruzione del ruolo assunto da ciascun attore all'interno del processo di progettazione, addestramento, nonché implementazione del sistema. Tale operazione è resa ulteriormente problematica dalla presunta autonomia decisionale dei sistemi basati su *machine learning*, i quali, in ragione della loro capacità di auto-apprendimento ed adattamento[3], vengono talvolta ritenuti - da parte della dottrina più ardita - idonei ad interrompere il nesso causale tra le scelte del programmatore e l'evento dannoso. Tuttavia, come noto, solamente eventi realmente imprevedibili ed inevitabili sono in grado di interrompere il nesso causale in ambito penalistico; al contrario, la c.d. "imprevedibilità genericamente prevedibile"[4] delle condotte algoritmiche, impone all'agente umano un dovere rafforzato di prevenzione e di gestione del rischio, rendendo fragile la distinzione tra errore tecnico e colpa giuridicamente rilevante.

[3] S. RUSSELL- P, NORVIG, *Artificial Intelligence: A Modern Approach*, Pearson College Div., 4th ed., 2020, p. 651 ss.
[4] C. PIERGALLINI, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?* cit., p. 1762.

L’autonomia decisionale dell’IA: *machina delinquere non potest*

All’interno del dibattito giuridico contemporaneo, l’autonomia decisionale dei sistemi di intelligenza artificiale viene spesso evocata come possibile base per ipotizzare una responsabilità diretta della macchina rispetto agli illeciti che essa contribuisce, in tutto o in parte, a realizzare.[1] Tuttavia, tale approccio rischia di generare una pericolosa ambiguità concettuale, soprattutto in ambito penalistico, ove il concetto di responsabilità è indissolubilmente legato a categorie antropocentriche, quali volontà, consapevolezza e colpevolezza.

Il diritto penale, più di ogni altro settore dell’ordinamento, è stato originariamente concepito per le persone fisiche, in quanto unicamente l’essere umano è ritenuto capace di autodeterminazione, colpevolezza, nonché meritevolezza della pena. In tale prospettiva, l’idea che una macchina possa essere ritenuta penalmente responsabile per le proprie azioni entra in diretto contrasto con un principio implicito, bensì profondamente radicato nel diritto penale: *machina delinquere (et puniri) non potest*. Parafrasando la storica formula che un tempo escludeva la responsabilità penale delle persone giuridiche -*societas delinquere non potest*- si potrebbe oggi affermare che l’ordinamento penale, non riconosce - né in astratto né in concreto - alcuna soggettività giuridico-penale autonoma alle intelligenze artificiali, ai robot, ovvero ai sistemi algoritmici.

Pertanto, anche nell’ipotesi in cui un sistema di intelligenza artificiale realizzi materialmente una condotta astrattamente sussumibile in una fattispecie incriminatrice, l’ordinamento giuridico non prevede alcuna forma di responsabilità penale diretta in capo alla macchina, riconducendo al più tale evento, ad una forma di responsabilità mediata o vicaria dell’essere umano, secondo uno schema imputativo e consolidato nella dogmatica penalistica. Invero, in tale modello, il sistema artificiale è qualificabile come mero strumento nelle mani del vero autore del fatto.[6]

[5] Il principale teorizzatore della possibile configurazione di una responsabilità penale diretta in capo ai sistemi di intelligenza artificiale, è il penalista israeliano Gabriel Hallevy, vd. G. HALLEVY, *Liability for Crimes Involving Artificial Intelligence Systams*, Springer, 2015.

[6] Per tutti, cfr. PAGALLO, The adventures of Picciotto Roboto, p. 352-353.

D’altra parte, fino ad oggi, nessun ordinamento giuridico ha riconosciuto validamente una forma di imputabilità penale autonoma in capo ai sistemi di intelligenza artificiale stessi. Al contrario, ogni ricostruzione penalmente rilevante delle condotte illecite ascrivibili all’azione, ovvero all’omissione, di un sistema intelligente continua a passare necessariamente attraverso l’azione o l’omissione dell’agente, nella sua qualità di soggetto imputabile, consapevole e colpevole.

Alla luce di ciò, l’autonomia decisionale dell’intelligenza artificiale, pur avendo una rilevanza tecnica ed operativa, non può essere giuridicamente intesa come fonte di responsabilità autonoma, almeno fintanto che essa non sia accompagnata da una rivoluzione concettuale che ridefinisca le fondamenta stesse del diritto penale, la cui struttura resta, ad oggi, inscindibilmente antropocentrica.

PROFILI DI RESPONSABILITÀ PENALE DELLA PERSONA FISICA

Le figure del *provider* e del *deployer*

Nel tentativo di tracciare i contorni della responsabilità penale connessa all'impiego di sistemi di intelligenza artificiale, assumono rilevanza primaria le figure del *provider* e del *deployer,* come qualificate dal Regolamento (UE) 1689/2024, anche noto AI Act[7].

Il *provider* è il soggetto che progetta, sviluppa o fa sviluppare un sistema di IA sotto la propria responsabilità, assumendosi l'onere di garantirne la conformità sin dalla fase genetica[8]. A tale figura competono, pertanto, obblighi di natura sostanzialmente tecnico-progettuale, che si riflettono sulla struttura, sulla finalità e sulle garanzie di sicurezza del sistema stesso, prima ancora che esso venga messo in esercizio.

Il *deployer*, per converso, è colui che, nell'ambito della propria attività professionale o istituzionale, immette in funzione il sistema, determinandone concretamente le modalità applicative e assumendone il controllo operativo ed incidendo direttamente sulla interazione con l'ambiente fattuale in cui viene utilizzato[9].

La distinzione concettuale e normativa tra tali figure non riveste unicamente rilievo classificatorio, bensì costituisce un nodo ermeneutico essenziale nell'analisi dei profili di imputazione soggettiva e nella determinazione dei criteri di attribuzione della responsabilità penale. Invero, la natura strutturalmente differente delle attività rispettivamente svolte da *provider* e *deployer* determina un diverso grado di incidenza causale nella genesi dell'evento lesivo, nonché una disomogeneità nelle rispettive sfere di dominio dell'azione, secondo quanto prescritto dai principi di colpevolezza e dell'offensività.

[7] Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione, COM/2021/206 finale, 21 aprile 2021 (c.d. AI Act).

[8] Parlamento Europeo e Consiglio dell'Unione Europea (2024). *Regolamento (UE) 2024/1689 sull'intelligenza artificiale* (AI Act), art. 3, comma 3. Gazzetta Ufficiale dell'Unione Europea.

[9] Parlamento Europeo e Consiglio dell'Unione Europea (2024). *Regolamento (UE) 2024/1689 sull'intelligenza artificiale* (AI Act), art. 3, comma 4. Gazzetta Ufficiale dell'Unione Europea.

Responsabilità dolosa e data machine training

Nel panorama delle responsabilità penalmente rilevanti connesse all'impiego di sistemi di intelligenza artificiale, l'ipotesi di utilizzo doloso dell'IA solleva profili di particolare interesse, soprattutto con riguardo al processo di data machine training, ossia quella fase essenziale nella quale l'algoritmo viene istruito mediante l'elaborazione di ingenti quantità di dati.

In questo contesto, la qualità, la completezza, nonché la veridicità dei dati impiegati, assumono rilievo dirimente nella determinazione dell'affidabilità e della correttezza dei risultati generati dal sistema. Invero, un intervento intenzionalmente manipolatorio su tali *dataset* configura condotte dolose nelle quali la macchina, lungi dall'essere soggetto autonomo, si rivela strumento operativo dell'agente umano.

Pertanto, la dottrina penalistica più avvertita non esita a riconoscere che, nell'ambito delle fattispecie dolose, l'imputazione soggettiva non incontra particolari ostacoli teorici, poiché l'intento antigiuridico consapevolmente perseguito, permane il centro nevralgico dell'illecito, rendendo irrilevante la natura – tradizionale o tecnologicamente avanzata – del mezzo adoperato per la realizzazione del reato. In questa ottica, il sistema intelligente rimane *instrumentum scleris*, veicolo esecutivo dell'input criminoso formulato a monte [10].

Tuttavia, la crescente sofisticazione dei sistemi intelligenti, nonché l'insidiosità tecnica che essi possono manifestare in ragione delle loro modalità di impiego, ha indotto il legislatore ad intervenire sul piano normativo, con l'introduzione dell'Atto del Senato n.1146, attualmente ancora in fase di approvazione. Precisamente, il Disegno di Legge all'art. 26 comma 1, lett. a) prevede l'introduzione di una circostanza aggravante comune, applicabile a qualunque fattispecie di reato, qualora lo stesso sia commesso mediante l'utilizzo di sistemi di intelligenza artificiale che, per natura o modalità operative, abbiano costituito mezzo insidioso, ostacolato la pubblica o privata difesa, ovvero aggravato le conseguenze del reato.

[10] P. SEVERINO, Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale, in P. SEVERINO (a cura di), Intelligenza artificiale, politica, economia, diritto, tecnologia, Luiss Uni Press, 2022.

Tale previsione normativa, oltre a costituire un significativo indice del crescente riconoscimento della rilevanza penale dell'impiego doloso dei sistemi di intelligenza artificiale, impone una rinnovata attenzione alla valutazione dell'elemento soggettivo del reato, nonché alla pericolosità oggettiva del mezzo utilizzato.

Responsabilità penale colposa del *provider* e del *deployer*

Nel vigente assetto normativo, la tematica della responsabilità penale colposa connessa all'impiego di strumenti fondati su intelligenza artificiale, impone una riflessione dogmaticamente strutturata, imperniata alle due figure di *provider* e *deployer*.

Per quanto attiene alla figura del *provider*, il piano della responsabilità penale si innesta, anzitutto, in un quadro riconducibile alle categorie della colpa da prodotto difettoso e della colpa nell'esercizio di attività pericolosa, secondo paradigmi già noti alla dogmatica penalistica e al diritto europeo. L'intelligenza artificiale, in particolare nelle sue declinazioni a più elevata autonomia funzionale, integra per sua natura un'attività ad elevato rischio tecnologico. Pertanto, in questo contesto, il provider assume una posizione di garanzia qualificata *ex lege*, la cui fonte è rinvenibile non solo nei principi generali del diritto penale, ma anche nelle recenti previsioni dell'AI Act, il quale delinea obblighi di progettazione, validazione e monitoraggio a carico del produttore [11].

Tuttavia, la struttura ipercomplessa, stratificata e frammentata della filiera di sviluppo dei sistemi di intelligenza artificiale - spesso distribuita tra numerosi attori e segmentata in fasi iterative ed interdipendenti - rende estremamente arduo un accertamento causale lineare e sicuro, in particolare sotto il profilo della riconducibilità della condotta colposa al singolo evento lesivo. Invero, il *deficit* di trasparenza algoritmica, l'opacità delle architetture di *machine learning*, nonché l'imprevedibilità emergente nei comportamenti adattivi dell'intelligenza artificiale, generano una vera e propria *black box* decisionale, ostativa al principio di tassatività e alla personalità della responsabilità penale.

In tale prospettiva, la responsabilità colposa del *provider* potrà ritenersi sussistente soltanto allorché sia accertabile, con rigore probatorio, la violazione di obblighi cautelari specifici, fondati su normative settoriali, linee guida tecniche, standard industriali riconosciuti e *best practices* consolidate[12].

[11] Parlamento Europeo e Consiglio dell'Unione Europea (2024). Regolamento (UE) 2024/1689 sull'intelligenza (AI Act), art. 25. Gazzetta Ufficiale dell'Unione Europea.
[12] I. SALVADORI, Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, 2021. P. 83.

In altri termini, la colpa penalmente rilevante dovrà coincidere con una sottovalutazione grave ed ingiustificata del rischio residuo, ossia con una condotta negligente od imprudente, idonea a travalicare la soglia del rischio consentito, la cui delimitazione sarà affidata alle norme cautelari tecniche e regolamentari, vere e proprie fonti di concretizzazione del dovere di diligenza tecnologica. Invero, in assenza di una tale condotta connotata da *blameworthiness*, non potrà configurarsi un giudizio di rimproverabilità soggettiva coerente con i principi di offensività, proporzionalità e colpevolezza.

Diverso, ma non meno problematico, è il versante della responsabilità penale colposa del *deployer*, la cui posizione di garanzia, ancor più rispetto a quella del *provider*, dipende strettamente da future scelte legislative circa la natura e l'ampiezza del dovere di controllo che gli sarà attribuito. La ratio sottesa alla disciplina europea impone infatti, in linea generale, che ogni attività potenzialmente lesiva di diritti fondamentali, sia svolta sotto il controllo umano significativo, c.d. *human oversight*. Tuttavia, tale impostazione rischia di generare un control dilemma di natura penalistica, poiché il *deployer,* pur formalmente titolare di un potere impeditivo, si trova spesso dinanzi a sistemi autonomi il cui funzionamento interno – basato su apprendimento automatico, adattività ed auto-ottimizzazione – è per lui inintelligibile, imprevedibile e, nei casi limite, non dominabile. Pertanto, si rischierebbe in questa maniera di attribuire una responsabilità di posizione a fronte di un potere meramente nominale ed ineffettivo, con conseguente stravolgimento del principio personalistico di colpevolezza, così come della funzione garantista del diritto penale. Conseguentemente, per evitare che l'operatore divenga un mero capro espiatorio, occorrerà limitare l'imputazione soggettiva della colpa ai soli casi di grave negligenza od omissione qualificata[13].

[13] Sul tema della legalità della colpa, cfr. F. GIUNTA, *La legalità della colpa*, In Criminalia, 2008, p.14

RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI EX D.LGS. 231/2001

Introduzione

La disciplina introdotta dal D.lgs. 231/2001 segna un superamento dell'impostazione personalistica che ha storicamente permeato il diritto penale, sancendo l'ingresso di una forma autonoma di responsabilità in capo agli enti collettivi. Invero, non si tratta più di una derivazione automatica della condotta del soggetto agente, bensì del riconoscimento di un disvalore proprio dell'ente, radicato nelle scelte organizzative e gestionali che ne connotano l'identità. Pertanto, l'illecito imputabile alla persona giuridica, non si esaurisce nella mera proiezione del reato commesso dalla persona fisica, ma assume la fisionomia di una responsabilità strutturale, fondata sulla mancata adozione – o sull'inefficace attuazione – di modelli idonei a prevenire la commissione di reati: è la cosiddetta *colpa di organizzazione*, cifra distintiva di un sistema che valorizza la prevenzione come strumento di tutela penale anticipata.

In tale prospettiva, il fulcro della disciplina è costituito dalla capacità dell'ente di dotarsi di un apparato strutturale e procedurale che sia idoneo a prevenire[14] la commissione di reati da parte dei propri esponenti. Invero, non è sufficiente che il reato sia commesso da un soggetto apicale [15] o subordinato nell'interesse o a vantaggio dell'ente, c.d. criterio oggettivo; occorre altresì verificare se l'organizzazione fosse adeguatamente predisposta per intercettare o prevenire la condotta illecita, c.d. criterio soggettivo.

A tal fine, l'adozione e l'efficace attuazione di un modello di organizzazione, gestione e controllo assume valore esimente per l'ente, ma solo se si dimostra che esso sia stato effettivamente applicato nella realtà aziendale, costantemente aggiornato, sorvegliato da un organismo autonomo ed indipendente[16].

[14] E. AMATI, N. MAZZACUVA, *Diritto penale dell'economia*, p. 58.
[15] Più precisamente si tratta di soggetti dotati di poteri di rappresentanza o di direzione dell'ente, ovvero di unità organizzative con autonomia funzionale e finanziaria. E. N. Mazzacuva, *Diritto penale dell'economia*, Milano, 2023, p. 47.
[16] L. Parodi, *Illecito penale dell'ente e colpa di organizzazione. Una recente conferma della traiettoria garantista tracciata dalla giurisprudenza di legittimità*, in Sistema Penale, 2023.

Tale assetto è oggi posto sotto forte pressione dall'irruzione dei sistemi di intelligenza artificiale nei processi decisionali d'impresa. Infatti, l'utilizzo di algoritmi, potenzialmente opachi nei criteri ed imprevedibili nei risultati, rischia di alterare le dinamiche tradizionali di imputazione e vigilanza, introducendo elementi di delega tecnologica, che sfuggono ai consueti presidi organizzativi. Pertanto, si impone una riflessione circa la necessità di adattare i modelli 231 affinché contemplino e disciplinino l'impiego di sistemi intelligenti, estendendo la *compliance* anche ai rischi derivanti dall'automazione decisionale. In tal senso, l'adeguatezza del modello non potrà più prescindere da una *digital risk assessment* che individui le aree di esposizione generate dall'integrazione dell'IA nei processi aziendali, né da un aggiornamento delle misure di controllo idonee a presidiare tali nuove frontiere del rischio penale.

Il modello organizzativo

Il modello organizzativo, nella prospettiva delineata dal D.lgs. 231/2001, non costituisce un mero apparato procedurale, bensì un presidio dinamico[17], finalizzato a prevenire la commissione di illeciti attraverso una razionale organizzazione dell'attività d'impresa. La sua efficacia, in termini esimenti o attenuanti della responsabilità dell'ente, è subordinata alla presenza di requisiti sostanziali, espressamente indicati agli artt. 6 e 7 del decreto. All'interno di tale novero, rilevano la mappatura delle aree di rischio, l'adozione di protocolli per disciplinare i processi decisionali, la gestione trasparente delle risorse finanziarie, l'istituzione di obblighi informativi verso l'Organismo di Vigilanza, nonché l'introduzione di un apparato sanzionatorio interno per reprimere le violazioni.

Tale struttura deve inoltre prevedere procedure di verifica periodica della propria attualità ed efficacia, nonché strumenti atti a consentirne l'adattamento sistemico a mutamenti normativi, organizzativi o tecnologici. Ed è proprio su quest'ultimo fronte che si colloca, oggi, una delle più pressanti sfide interpretative ed applicative: l'integrazione dei sistemi di intelligenza artificiale nei processi aziendali.

L'ingresso strutturato dell'IA nell'operatività delle imprese comporta l'emersione di nuovi profili di rischio penale, talvolta di natura del tutto inedita. In tale contesto, i modelli organizzativi sono chiamati ad evolversi, accogliendo presìdi specifici volti a regolare l'uso responsabile e conforme delle tecnologie intelligenti. Le modifiche normative *in itinere* – e, in particolare, il Disegno di Legge sull'intelligenza artificiale – impongono un ripensamento profondo dell'architettura della *compliance*, sia in chiave preventiva che repressiva, richiedendo al legislatore delegato di ridefinire, anche sotto il profilo sostanziale e processuale, i criteri di imputazione della responsabilità amministrativa degli enti in relazione agli illeciti commessi mediante IA, tenendo conto del grado di controllo effettivamente esercitabile sui sistemi utilizzati.

[17] E. AMATI, N. MAZZACUVA, *Diritto penale dell'economia*, p. 60.

Pertanto, ciò impone un'estensione della responsabilità organizzativa anche a condotte che, pur materialmente poste in essere da entità non imputabili – come *software* autonomi o modelli predittivi – siano tuttavia riconducibili, in termini di colpa di organizzazione, a lacune nella *governance* aziendale.

La transizione digitale e l'avvento dell'IA sono, quindi, da considerarsi fattori idonei a riconfigurare la responsabilità d'impresa, da ciò discendendo la necessità di strutturare e/o ristrutturare i modelli organizzativi affinché possano essere valutati idonei a gestire non solo i rischi "classici", ma altresì i nuovi scenari di rischio derivanti dall'adozione di tecnologie autonome ed auto-apprendenti, in un'ottica di compliance anticipatoria e adattiva.

Risk assessment

La stesura del modello organizzativo esige una conoscenza penetrante ed articolata dell'ente, che abbracci la sua struttura organica, l'assetto funzionale, le prerogative degli organi direttivi, nonché l'oggetto sociale nel suo complesso. Soltanto a partire da tale consapevolezza si potrà procedere ad una puntuale e rigorosa mappatura delle aree a rischio di commissione di illeciti, la quale si traduce in una valutazione di natura statistico-probabilistica, fondata sull'elaborazione e l'analisi sistematica dei dati rilevanti.

La transazione e l'evoluzione digitale in argomento comportano la necessità per gli enti di rivedere e potenziare le attività di risk assessment, affinché contemplino, in modo esplicito, le criticità ed i rischi connessi all'uso dell'intelligenza artificiale.

Il fulcro della problematica risiede nella disamina dei vantaggi e delle criticità insiti nella compliance digitale, nonché nelle implicazioni che l'adozione di tali strumenti tecnologici comporta in ordine all'attribuzione della responsabilità amministrativa degli enti. In particolare, l'introduzione e l'impiego di sistemi di intelligenza artificiale richiedono un ampliamento dell'orizzonte valutativo tradizionale, poiché essi possono accentuare la complessità del rischio, introducendo elementi di opacità, autonomia decisionale e potenziale amplificazione delle conseguenze illecite.

Di conseguenza, il processo di *risk assessment* dovrà necessariamente inglobare una dimensione di analisi digitale, volta ad identificare e ponderare i rischi specifici derivanti dall'utilizzo di tali tecnologie, al fine di garantire che il modello organizzativo mantenga la propria efficacia preventiva anche nella nuova frontiera dell'automazione e dell'intelligenza algoritmica.

Codice etico e sistemi di intelligenza artificiale

Il rafforzamento dei presidi 231 si estende, altresì, al Codice Etico ex art. 6, comma 3 del D.Lgs. 231/2001 che, come noto, rappresenta l'espressione valoriale e comportamentale dell'identità dell'ente, fungendo da parametro interno di legalità e da presidio culturale della *compliance*. Invero, nell'epoca della trasformazione digitale, esso dovrà accogliere, in maniera espressa e sistematica, principi di integrità, trasparenza e responsabilità applicabili all'impiego di tecnologie intelligenti. In questa prospettiva, l'inserimento nel codice etico di disposizioni specifiche relative all'uso di intelligenza artificiale, costituisce non soltanto una misura di prevenzione conforme alla ratio del decreto, ma anche una manifestazione dell'impegno etico dell'ente nel governare con consapevolezza i rischi derivanti dall'automazione. Il codice, così aggiornato, assume una funzione proattiva nella costruzione di una cultura aziendale improntata al rispetto della legalità sostanziale, anche nelle nuove dimensioni dell'agire digitale.

GEBBIABORTOLOTTO

PENALISTI ASSOCIATI

Corso Vittorio Emanuele II, 68
10121 – Torino
Telefono +39 011 4546389
segreteria@gbpenalisti.it