GIURISPRUDENZA PENALE

L'impatto dell'Intelligenza Artificiale sui Modelli 231 e sui sistemi di *compliance* aziendale alla luce delle novità introdotte dal DDL sull'AI.

di ***Davide Costa***

Sommario: 1. Premessa. I Modelli Organizzativi e la normativa europea e nazionale sull'Intelligenza Artificiale – **2.** Le aggravanti: una disciplina rafforzata dal DDL sull'intelligenza artificiale. – **3.** Verso nuovi reati presupposto. – **4.** Conclusioni: un nuovo paradigma per la *compliance* aziendale.

1. Premessa. I Modelli Organizzativi e la normativa europea e nazionale sull'Intelligenza Artificiale

L'introduzione dell'intelligenza artificiale nei contesti e nelle procedure aziendali non rappresenta solo un'importante evoluzione tecnologica e un'innegabile agevolazione pratica nello svolgimento di plurime mansioni quotidiane, ma, soprattutto, una trasformazione sistemica che incide in profondità sull'organizzazione del lavoro, sulle filiere produttive e, in maniera sempre più evidente, sul sistema dei rischi legati alla compliance.

L'IA sta ridefinendo non solo i processi operativi e i modelli decisionali, ma anche le dinamiche interne tra ruoli, responsabilità e livelli di controllo. In tale contesto, cambia inevitabilmente anche lo scenario in cui possono maturare condotte illecite: l'utilizzo dell'intelligenza artificiale può, infatti, costituire un mezzo particolarmente insidioso per la commissione di reati, incidendo sull'opacità delle condotte, sull'amplificazione degli effetti offensivi e sull'elusione dei presidi di controllo.

Di fronte a questa evoluzione, l'adeguamento dei Modelli Organizzativi ex d.lgs. 231/2001 diventa un passaggio obbligato.

Com'è noto, il legislatore ha predisposto due criteri d'imputazione della responsabilità delle persone giuridiche.

Il primo è il criterio di imputazione oggettivo, previsto dall'art. 5 del D.Lgs. 231/2001, secondo cui l'ente risponde dell'illecito amministrativo in rilievo soltanto se il reato presupposto è stato commesso nel suo interesse od a suo vantaggio.

Il secondo, invece, è il criterio d'imputazione soggettivo, stabilito dall'art. 6 per i reati commessi da soggetti che rivestono posizioni apicali e dall'art. 7 per reati commessi dai sottoposti.

In virtù del criterio soggettivo, nel caso in cui soggetti attivi del reato presupposto siano apicali, l'ente, ai sensi dell'art. 6 del Decreto, non risponde dell'illecito amministrativo laddove venga fornita la prova:

- dell'adozione di un modello organizzativo e di gestione idoneo a prevenire la commissione di reati della stessa specie;
- dell'istituzione di un organismo di vigilanza indipendente con autonomi poteri di iniziativa e controllo;
- del fatto che non vi è stato un omesso controllo o un'insufficiente vigilanza dell'organismo di vigilanza;
- dell'elusione fraudolenta del modello di organizzazione e gestione da parte degli apicali, autori del reato presupposto.

Nel caso invece in cui il reato sia stato commesso da soggetti sottoposti, l'Ente è ritenuto responsabile se la commissione dello stesso è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Il Decreto stesso, inoltre, prevede che l'inosservanza degli obblighi di direzione e vigilanza debba essere esclusa se l'Ente, prima della commissione del reato, abbia adottato e abbia dato concreta attuazione ad un Modello di organizzazione e di gestione idoneo a prevenire reati della specie di quello verificatosi.

In altre parole, potrà addivenirsi all'esclusione di responsabilità dell'ente per reati presupposto commessi da apicali e/o sottoposti solo in assenza di una "colpa organizzativa"; colpa organizzativa la cui esclusione, sulla scorta dell'insegnamento dell'ormai nota sentenza della VI Sezione Penale della Corte di Cassazione, n. 23401 del 15/6/2022, c.d. "Impregilo", presuppone che nel modello sia stato valutato il rischio di commissione dei reati della stessa specie di quello compiuto e siano state predisposte valide misure volte ad evitare, o quantomeno minimizzare, il rischio della sua realizzazione [1].

Il Legislatore, ritenendo la prevenzione il miglior strumento per ridurre i rischi di commissione di reati, ha predisposto una disciplina che persegue l'obiettivo di indurre le persone giuridiche ad implementare la propria *compliance* nell'organizzazione aziendale, predisponendo regole di comportamento, procedure e sanzioni.

Affinché venga riconosciuto l'effetto premiale derivante dall'adozione del modello organizzativo, consistente nell'esenzione della responsabilità da reato o, nel caso in cui il modello sia adottato dopo la commissione dell'illecito, nell'attenuazione delle conseguenze sanzionatorie (ovvero, se la riforma del Decreto 231 tutt'ora in cantiere dovesse vedere la luce, l'estinzione del reato [2]), il modello stesso deve possedere delle caratteristiche specifiche.

---

[1] V. Sentenza Cass. Pen. VI Sez., n. 23401 del 15/6/2022, rinvenibile online su https://www.giurisprudenzapenale.com/wp-content/uploads/2022/06/cass-pen-2022-23401.pdf;

[2] Nel progetto di riforma del Decreto 231, in discussione nell'ambito del Tavolo Tecnico istituito dal Ministero della Giustizia con Decreto del 7/2/2025, è presente un'inedita procedura di estinzione dell'illecito amministrativo, e conseguente venir meno della responsabilità dell'ente, che prevede che l'ente stesso che, prima della commissione del reato, abbia adottato e attuato il modello di organizzazione secondo la struttura stabilita,

Gli artt. 6 e 7 del D.Lgs. 231/2001 tratteggiano, in chiave generale ed astratta, i caratteri che i modelli devono possedere per rispondere all'esigenza di:

- individuare le principali aree di rischio di commissione di reati;
- prevedere specifici protocolli per programmare la formazione ed attuazione delle decisioni in relazione ai reati da prevenire;
- individuare le modalità di gestione delle risorse economiche;
- prevedere obblighi di informazione periodici nei confronti dell'organismo di vigilanza;
- introdurre un sistema disciplinare volto a sanzionare la violazione delle procedure contenute nel modello.

L'art. 7, inoltre, fornisce una definizione specifica di efficace attuazione, stabilendo che nel modello devono essere previste delle procedure che consentano, periodicamente, l'agevole verifica della sua stessa attualità nonché le modalità per permettere la modifica sistematica delle procedure e di ogni inadeguatezza sopravvenuta.

Tuttavia, la disciplina dettata dal D.Lgs 231/2001, con riguardo agli aspetti strumentali, contenutistici ed istituzionali del modello, è, allo stato attuale, eccessivamente generica poiché non pone alcun criterio oggettivo che possa orientare il Giudice circa l'idoneità del modello e la sua colpa d'organizzazione. In conseguenza di tale deficit normativo di legalità e tassatività, il giudizio sul comportamento dell'ente e la valutazione dell'idoneità od inidoneità del modello è demandato all'esclusiva discrezionalità del giudicante, che, secondo i canoni interpretativi offerti dalla richiamata sentenza "Impregilo", dovrà tener in considerazione la specificità del modello e la sua calibrazione sulle specifiche caratteristiche dell'ente (dimensioni, tipo di attività, evoluzione diacronica), nonché l'adozione del modello stesso in conformità alla linee guida e ai codici di comportamento delle associazioni di categoria.

Alla luce di quanto detto, il modello deve essere pensato e strutturato appositamente per la società che lo adotterà, in considerazione di tutte le peculiarità dell'organizzazione aziendale, del *core business* e delle principali aree di rischio.

Se, pertanto, il Decreto consente all'ente di andare esente da responsabilità e "colpa di organizzazione" per reati commessi nel suo interesse o a suo vantaggio da soggetti apicali ovvero da sottoposti solo in presenza dell'adozione, e dell'efficace attuazione, di un modello di organizzazione, gestione e controllo idoneo a prevenire i reati presupposto, nonché del suo costante aggiornamento

---

può chiedere al giudice, entro trenta giorni dalla notifica dell'avviso di conclusione dell'indagine preliminare, un termine per **eliminare le carenze del modello** riscontrate dal pubblico ministero che hanno determinato o agevolato la commissione del reato. I dettagli della proposta di riforma sono meglio specificati nel Position Paper pubblicato da Confindustria nel marzo 2025, consultabile online a: https://www.dirittobancario.it/wp-content/uploads/2025/04/Position-Paper-Confindustria-marzo-2025.pdf

alla luce dell'evoluzione normativa, è facile comprendere che l'irruzione dell'IA nei meccanismi aziendali impone una revisione sostanziale di tali modelli, affinché siano realmente in grado di intercettare e neutralizzare i nuovi rischi di reato legati all'automazione e all'autonomia decisionale delle tecnologie emergenti.
D'altronde, i processi automatizzati, l'analisi dei dati, le decisioni affidate agli algoritmi trasformano il terreno su cui possono germogliare condotte illecite riconducibili a reati presupposto, quali il riciclaggio e l'autoriciclaggio (mediante strumenti automatizzati che rendano più difficile il tracciamento delle operazioni), le violazioni della proprietà intellettuale (quali l'utilizzo non autorizzato di opere protette da diritto d'autore, quali testi, immagini, musica o *software*, per l'addestramento di modelli di intelligenza artificiale, nonché la riproduzione, comunicazione al pubblico o diffusione online non autorizzata di opere dell'ingegno coperte da privativa attraverso tecnologie di IA), nonché le violazioni della normativa in materia di protezione dei dati personali, in particolare con riferimento alla raccolta massiva, al trattamento non conforme o alla profilazione automatizzata degli interessati. A questi si aggiungono i reati informatici, che possono essere agevolati o direttamente commessi tramite tecnologie basate sull'intelligenza artificiale, quali l'accesso abusivo a sistemi informatici o telematici, il danneggiamento di sistemi informatici, la creazione di malware o l'impiego di chatbot malevoli capaci di ingannare utenti e carpire credenziali sensibili. L'IA, come noto, può inoltre potenziare campagne di phishing automatizzato, elaborare tecniche di social engineering su larga scala o persino manipolare dati in tempo reale per eludere sistemi di sicurezza. Particolare attenzione merita, in tal senso, l'impiego dei *Large Language Models* (LLM), ovvero modelli di linguaggio di grandi dimensioni capaci di generare testi coerenti, persuasivi e personalizzati su vasta scala. Tali modelli, se utilizzati in modo malevolo, possono alimentare *chatbots* ingannevoli o automatizzare la produzione di comunicazioni fraudolente estremamente convincenti, aumentando l'efficacia degli attacchi informatici e la difficoltà nel rilevarli. In questo contesto, l'intelligenza artificiale non è solo un potenziale strumento del reato, ma può anche divenire l'ambiente stesso in cui si realizza la condotta illecita, rendendo necessario un rafforzamento delle strategie di prevenzione e di *compliance*.
Questo rende urgente un riesame dei modelli di organizzazione e gestione previsti dal d.lgs. 231/2001, oltreché, più in generale, delle *policy* e delle procedure interne, al fine di continuare a beneficiare della possibilità di esonero dalla responsabilità amministrativa in caso di reato.
Il modello 231 e le procedure aziendali di gestione del rischio devono quindi essere aggiornati in modo da:

- intercettare nuovi rischi di illecito connessi all'impiego di IA;
- integrare misure specifiche di controllo sull'uso degli algoritmi e sull'accesso ai sistemi, anche ai fini dell'impiego di dati di persone fisiche il cui trattamento è sottoposto alle tutele previste dal Regolamento UE 2016/679 (GDPR);

- rafforzare la formazione del personale sull'utilizzo sicuro e conforme dei sistemi e dei *tools* di intelligenza artificiale.

In un'ottica di *compliance* aziendale e di prevenzione dell'utilizzo dell'intelligenza artificiale quale mezzo per la commissione di reati in grado di impegnare la responsabilità dell'ente, assume particolare rilievo l'intervento normativo del Disegno di Legge in materia di Intelligenza Artificiale, già approvato in prima lettura al Senato (Atto Senato n. 1146), e attualmente in esame alla Camera (Atto Camera n. 2316) [3].

Trattasi della proposta legislativa, la prima in Europa, diretta ad adottare nell'ordinamento interno le disposizioni dell'ormai noto Regolamento UE 2024/1689 sull'intelligenza artificiale, o, nel linguaggio comune, AI Act [4]. L'obiettivo del DD., in tale ottica, è la promozione di "*un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità*" e l'introduzione di criteri regolatori, norme di principio e di settore, che promuovono l'utilizzo delle nuove tecnologie prevedendo, al contempo, misure in grado di contenere il rischio connesso al loro uso improprio o dannoso.

In questo nuovo scenario, i modelli organizzativi previsti dal d.lgs. 231/2001 devono, pertanto, essere rivisti e aggiornati. Le imprese sono dunque chiamate ad affrontare un adeguamento non solo tecnico ma anche normativo, alla luce delle novità introdotte dal citato disegno di legge sull'intelligenza artificiale.

La riforma, tra i suoi punti salienti, include la delega al Governo per la revisione del sistema sanzionatorio e, per quanto qui interessa, per l'introduzione di nuovi reati. In questo contesto, assume particolare rilievo l'introduzione di una serie di aggravanti applicabili anche ai reati presupposto previsti dal Decreto 231.

2. Le aggravanti: una disciplina rafforzata dal DDL sull'intelligenza artificiale

Come anticipato, il DDL sull'Intelligenza Artificiale interviene in modo incisivo sul fronte sanzionatorio, prevedendo, in primo luogo, l'introduzione di una **nuova aggravante comune**, applicabile a tutti i reati, inclusi, quindi, quelli rilevanti ai fini della responsabilità amministrativa degli enti.

L'art. 26, comma 1, lett. a), del disegno di legge, infatti, introduce all'art. 61 del codice penale il n. 11 *decies,* che contempla un'aggravante ad effetto comune che si configura ogni qual volta il reato è commesso mediante l'impiego di sistemi di intelligenza artificiale quando, per la loro natura o modalità d'uso, questi abbiano costituito un mezzo insidioso, abbiano ostacolato le attività di difesa (pubblica o privata), oppure abbiano aggravato le conseguenze del reato.

[3] Si riporta il testo del D.D.L. come approvato dal Senato, rinvenibile online su: https://www.senato.it/service/PDF/PDFServer/BGT/01449288.pdf

[4] Si riporta il testo del Regolamento UE 2024/1689, rinvenibile online su: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401689

Accanto a questa aggravante generale, il DDL prevede **aggravanti specifiche per alcuni reati presupposto**, che quindi avranno un impatto diretto sull'adeguamento dei modelli organizzativi 231. Si tratta, in particolare, di aggravanti ad effetto speciale che interessano i seguenti reati.

- **Aggiotaggio (art. 2637 c.c.):** per tale reato societario, contemplato dall'art. 25-ter, comma 1, lett. r), del d.lgs. 231/2001, il DDL introduce un'aggravante ad effetto speciale (reclusione da due a sette anni) se il fatto è commesso mediante sistemi di IA.
- **Manipolazione del mercato (art. 185 TUF)**: anche qui è prevista un'aggravante ad effetto speciale con sanzioni aumentate (reclusione da due a sette anni e multa da 25.000 a 6 milioni di euro) qualora la diffusione di notizie false o il compimento di operazioni simulate o altri artifici in grado di alterare sensibilmente il prezzo di strumenti finanziari vengano poste in essere mediante sistemi di intelligenza artificiale, con conseguente impatto sull'art. 25-sexies del d.lgs. 231/2001.

E' stata invece espunta l'aggravante ad effetto comune originariamente contemplata dalla prima bozza del DDL per i reati di **riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio (artt. 648-*bis*, 648-*ter* e 648-*ter*.1 c.p.), anch'essi** inseriti tra i reati presupposto della responsabilità dell'ente dall'art. 25-*octies* del d.lgs. 231/2001; per tali fattispecie, infatti, era stata inizialmente proposta un'aggravante di pena laddove il reato fosse commesso "*mediante l'impiego di sistemi di intelligenza artificiale*". Attualmente, pertanto, la commissione dei predetti delitti attraverso sistemi di IA sarà più aspramente sanzionata in virtù dell'applicazione dell'aggravante generale introdotta all'art. 61 n. 11 *decies* c.p., di cui s'è detto poc'anzi. Effettivamente, è ragionevole ipotizzare che l'aggravante in parola sarà suscettibile di larga applicazione per i reati aventi ad oggetto il reimpiego di proventi derivanti da reato. Tali delitti, infatti, ben si prestano ad essere commessi attraverso tecniche algoritmiche avanzate, quali le applicazioni di IA, in considerazione della particolare capacità di sistemi di intelligenza artificiale di mascherare l'origine illecita dei flussi finanziari mediante l'utilizzo di tecniche di anonimizzazione, movimentazione automatizzata e frammentazione delle transazioni, rendendo più complessa l'attività investigativa e ostacolando l'identificazione dei beneficiari finali e della provenienza delittuosa delle risorse.

3. Verso nuovi reati presupposto.

Un altro punto centrale del DDL riguarda l'introduzione, da un lato di nuove fattispecie di reato nelle quali l'utilizzo di sistemi di IA costituisce esso stesso elemento costitutivo del delitto e la previsione di una (futura) espansione del catalogo dei reati presupposto.

Sotto il primo aspetto, il DDL introduce nell'ordinamento due nuove ipotesi di reato.

Un primo reato, introdotto dall'art. 26 c. 1 lett. c) del DDL, verosimilmente destinato a trovare un'amplia applicazione, e finalizzato a ricondurre ad una specifica fattispecie delittuosa una condotta oggi sempre più diffusa, è quello di cui all'art. 613 *quater* c.p., rubricato "illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale. La norma punisce con la reclusione da uno a cinque anni chiunque 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. Si tratta, in breve, di condotte che hanno ad oggetto la creazione, a scopo di arrecare pregiudizio, del c.d. "*deep fake*", meglio definito dall'art. 3 dell'AI Act come "*un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona*". È indubitabile che questa nuova ipotesi di reato contro la persona rappresenta una risposta necessaria e tempestiva a una nuova forma di aggressione che, grazie alla diffusione e all'accessibilità degli strumenti di intelligenza artificiale, sta assumendo proporzioni sempre più allarmanti. La norma riconosce la gravità dei danni, spesso irreparabili, che possono derivare dalla diffusione illecita di contenuti audiovisivi falsificati, tutelando la dignità, la reputazione e l'identità personale delle vittime. In un contesto in cui le tecnologie generative consentono con estrema facilità la creazione di immagini, voci e video verosimili ma artefatti, è fondamentale che l'ordinamento preveda una tutela penale efficace e mirata, atta a dissuadere comportamenti che minano profondamente la fiducia nelle relazioni digitali e nella veridicità dell'informazione.

L'art. 26, comma 3, inoltre, prevede l'ingresso, tra i reati contro il diritto d'autore contemplati dall'art. 171 L. 633/1941, di una nuova fattispecie alla lett. a-*ter*) del primo comma della norma, che punisce chi riproduce o estrae testi o dati da opere o materiali disponibili in rete o da banche dati, in violazione delle eccezioni consentite dagli artt. 70-ter e 70-quater, anche tramite sistemi di intelligenza artificiale. L'introduzione di questa previsione, secondo una prima lettura, risponde alla necessità di contrastare l'uso improprio dell'IA nei processi di *scraping* e *text/data mining* non autorizzati, che attraverso l'impiego di strumenti di IA possono avvenire su larga scala e con modalità tali da eludere i controlli ordinari. L'impiego di sistemi automatizzati consente infatti di acquisire e rielaborare enormi volumi di contenuti protetti da diritto d'autore, ponendo in seria crisi il sistema delle licenze e delle tutele patrimoniali e morali degli autori, e rendendo difficile sia la tracciabilità della violazione sia l'individuazione del soggetto responsabile.

Va detto, tuttavia, che, benché indubbiamente suscettibili di essere poste in essere in contesti societari ed a vantaggio o nell'interesse dell'ente, nessuna delle due fattispecie di nuova introduzione sembra destinata quantomeno alla data odierna, a determinare l'insorgenza di responsabilità per gli Enti, in assenza di specifica disposizione che faccia confluire i due delitti nel novero delle ipotesi di reato-presupposto previste rispettivamente dall'art. 25-*novies* D. Lgs. 231/1001 per i reati

contro il diritto d'autore e dall'art. 25-*quinquies* per i reati contro la personalità individuale.
Norma che, invece, è ad oggi prevista nel catalogo dei reati del Decreto 231 e che, in virtù del DDL, potrà trovare maggiore applicazione è costituita dall'art. 171-*ter* della L. 633/1941.
Ed infatti, per effetto dell'estensione, operata dall'art. 24 del DDL, della definizione di "opera dell'ingegno" di cui all'art. 1 della Legge sul Diritto d'Autore anche alle opere create con l'ausilio di intelligenza artificiale, ricadranno sotto la tutela penale del citato art. 171-*ter,* e, ai fini della responsabilità amministrativa degli Enti dell'art. 25-*novies* del Decreto 231, le condotte aventi ad oggetto la duplicazione, la diffusione o la riproduzione abusiva a fini di lucro di opere create con l'ausilio o il supporto di sistemi di intelligenza artificiale, oggi sempre più diffuse.
Di maggiore interesse, ai fini della *compliance* 231, è invece l'art. 22 del disegno di legge; esso, infatti, delega il Governo ad armonizzare la normativa interna con il Regolamento UE 2024/1689 sull'intelligenza artificiale.
In particolare, il comma 5, lett. b), del citato art. 22, assegna al legislatore il compito di introdurre nuove fattispecie penali, sanzionate anche a titolo di colpa, incentrate sull'omissione di misure di sicurezza nella progettazione, nella produzione e nell'uso professionale dell'IA, qualora tale omissione comporti un pericolo concreto per la vita, la sicurezza individuale o collettiva o per la sicurezza dello Stato. A ciò si aggiunge un ulteriore, significativo elemento di prospettiva: tale delega, se letta con l'attenzione rivolta ai principi espressi dall'AI Act, potrebbe infatti condurre alla criminalizzazione delle violazioni degli obblighi posti a carico dei soggetti destinatari del medesimo Regolamento UE 1689/2024. Quest'ultimo impone, tra l'altro, stringenti doveri di trasparenza, accuratezza, documentazione, sorveglianza post-commercializzazione e gestione del rischio a carico di fornitori, distributori, importatori e utilizzatori di sistemi di intelligenza artificiale, in particolare di quelli ad alto rischio.
In tale ottica, potrebbe trovare sanzione penale anche l'impiego o l'immissione sul mercato di sistemi di IA classificati come a rischio inaccettabile, e pertanto espressamente vietati dall'art. 5 del Regolamento (es. sistemi di manipolazione subliminale, social scoring da parte delle autorità pubbliche, o sistemi di identificazione biometrica in tempo reale in spazi pubblici, salvo eccezioni strettamente regolamentate).
Sarà dunque di estremo interesse osservare in quali specifici reati verrà tradotta questa ampia delega, e sarà cruciale la definizione dei criteri di imputabilità soggettiva, anche in rapporto al livello di consapevolezza e controllo effettivo del soggetto sull'uso della tecnologia. In particolare, l'ampio contenuto della delega lascia trasparire la possibilità che, un domani, il nostro ordinamento accoglierà non solamente fattispecie penali che sanzionano l'impiego illecito dell'intelligenza artificiale, come nel caso già previsto dei "*deepfake*" o dell'aggravante di cui all'art. 61 n. 11 *decies* c.p., ma anche reati volti a colpire direttamente la produzione, la commercializzazione e la diffusione di sistemi di IA in sé illeciti, perché vietati o

qualificati a rischio inaccettabile dal Regolamento UE 1689/2024. Si delinea così un possibile doppio binario sanzionatorio: da un lato, l'uso distorto di strumenti leciti; dall'altro, la realizzazione o messa in circolazione di strumenti vietati ab origine per la loro intrinseca pericolosità.
E' verosimile, peraltro, che tali reati, una volta introdotti, andranno ad allargare il novero delle fattispecie presupposto della responsabilità degli enti.
La lettera c) del medesimo comma 5, invero, apre alla possibilità di includere gli illeciti inerenti all'IA tra i reati presupposto ai sensi del D.Lgs. 231/2001, tenendo conto del grado di controllo esercitato dall'ente sul sistema. Ciò, per riallacciarsi a quanto esposto nelle battute iniziali del presente contributo, comporterà per le società l'obbligo di aggiornare i propri modelli organizzativi e di gestione, integrando la valutazione dei rischi specifici legati all'uso dell'intelligenza artificiale, in linea con le tipologie di rischio (minimo, limitato, alto o inaccettabile) delineate dall'AI Act. Si prospetta, dunque, un nuovo scenario normativo in cui la *compliance* tecnologica si fonderà con la responsabilità penale, imponendo agli operatori economici un adeguamento tanto tecnico quanto giuridico.

4. Conclusioni: un nuovo paradigma per la *compliance* aziendale

L'ingresso dell'intelligenza artificiale nell'impresa comporta una trasformazione che tocca tanto le dinamiche operative aziendali quanto gli assetti di responsabilità. L'adozione di tecnologie basate su IA può infatti generare, accanto a indubbi vantaggi competitivi, anche nuovi rischi legati alla possibilità che tali strumenti vengano utilizzati, anche inconsapevolmente, per la commissione di reati.
Questi scenari impongono alle imprese un'attenta riflessione sull'integrazione dell'IA nei processi aziendali, richiedendo l'adozione di misure organizzative e tecniche adeguate a prevenire responsabilità dirette e indirette derivanti dall'uso delle nuove tecnologie.
Una volta tramutato in legge, il DDL sull'IA, introducendo nuove aggravanti, fattispecie penali e obblighi di controllo, imporrà alle imprese un profondo ripensamento dei modelli organizzativi e gestionali. In parallelo, l'entrata in vigore del Regolamento UE 1689/2024 (AI Act) rafforza ulteriormente l'esigenza di adeguamento, introducendo un articolato sistema di classificazione dei rischi e obblighi specifici per fornitori, importatori, distributori e utilizzatori di sistemi di IA, soprattutto se ad alto rischio.
Di conseguenza, appare auspicabile che i modelli organizzativi vengano aggiornati non solo per rispondere al nuovo quadro sanzionatorio nazionale, ma anche per recepire puntualmente le previsioni del Regolamento europeo, integrando, laddove opportuno e tenuto conto del core business della società interessata, nel sistema di compliance aziendale le prescrizioni normative in materia di governance dei dati, documentazione tecnica, trasparenza, gestione del rischio e sorveglianza post-commercializzazione. Sarà quindi necessario un approccio integrato, che coniughi gli obblighi previsti dal D.Lgs. 231/2001 con quelli imposti dall'AI Act, in un'ottica di piena conformità normativa e responsabilità d'impresa.

Queste innovazioni normative rafforzano, evidentemente, la necessità per le imprese di predisporre adeguate misure di prevenzione e controllo, aggiornando tempestivamente i propri MOG, per rispondere al nuovo quadro sanzionatorio e adeguare i propri modelli di organizzazione e gestione in funzione della prevenzione di illeciti che potrebbero essere posti in essere proprio mediante l'impiego, anche improprio o negligente, di sistemi di intelligenza artificiale.
In particolare, maggiore attenzione dovrà essere dedicata alle Parti speciali dei Modelli, destinate ad essere integrate con la descrizione della struttura dei reati presupposto e delle nuove ipotesi aggravate commesse mediante strumenti di IA, nonché con l'identificazione delle aree di rischio e la valutazione del grado di pericolo con riferimento all'utilizzo di sistemi di intelligenza artificiale nelle differenti aree di attività aziendale.
Aggiornare il modello 231, rivedere i codici etici e i protocolli di prevenzione non appare più un'azione facoltativa ma un'esigenza di sistema. A questo processo di adeguamento deve affiancarsi un percorso formativo strutturato, volto a sensibilizzare tutte le figure aziendali sui rischi legati all'uso dell'IA e sulle responsabilità che ne derivano.
Inoltre, accanto alla formazione, sarà fondamentale l'adozione di comportamenti virtuosi e strumenti di governance tecnologica, in grado di prevenire l'abuso o l'uso improprio dell'intelligenza artificiale. Tra questi, l'istituzione di comitati etici per la valutazione dell'impatto dei sistemi di IA, l'introduzione di procedure interne per la verifica della conformità ai requisiti normativi (come la tracciabilità dei dati utilizzati per l'addestramento, il controllo dell'accuratezza e della robustezza degli algoritmi, l'adozione di misure di sorveglianza post-marketing), la nomina di una figura professionale competente per garantire la conformità normativa in materia di intelligenza artificiale (eventualmente estendendo in tale direzione le funzioni del DPO, se già presente), nonché l'implementazione di sistemi di audit e monitoraggio continuo sull'uso delle tecnologie intelligenti, per intercettare tempestivamente eventuali deviazioni o profili di rischio.
In quest'ottica, pur non essendoci ancora indicazioni o linee guida da parte delle associazioni di categoria in riferimento alle *best practices* in termini di *compliance* per l'uso di sistemi di IA, si apre anche l'opportunità di adottare sistemi di gestione strutturati per l'uso responsabile dell'intelligenza artificiale, quali quello previsto e certificato dallo standard ISO/IEC 42001, il primo standard internazionale specificamente dedicato ai sistemi di gestione dell'IA, il quale stabilisce i requisiti per creare, implementare, mantenere e migliorare continuamente un sistema di gestione dell'intelligenza artificiale.