ALERT MEMORANDUM

La nuova legge italiana sull'IA: la prima normativa nazionale nella UE che affianca l'AI Act

29 ottobre 2025

Con l'entrata in vigore, lo scorso 10 ottobre, della nuova Legge n. 132/2025 ("***Legge italiana sull'IA***"), l'Italia diventa il primo stato membro della UE a dotarsi di una legge quadro organica sullo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale ("***IA***"). La legge, che richiama il Regolamento europeo noto come ***AI Act*** (Regolamento UE 2024/1689), attribuisce al Governo ampie deleghe per l'attuazione dei principi e la definizione delle regole operative in essa enunciati, delineando al tempo stesso la struttura istituzionale cui sarà affidata la *governance* chiamata a orientare, coordinare e vigilare questo settore strategico per il futuro del Paese.

Le principali novità introdotte riguardano:

- l'individuazione delle autorità nazionali per l'intelligenza artificiale;
- la tutela del diritto d'autore anche quando le opere siano create con l'ausilio di strumenti di IA, purché risultato del lavoro intellettuale dell'autore;
- l'esplicita estensione delle eccezioni di *Text and Data Mining* ai sistemi di IA, a condizione che sia rispettato l'*opt-out* del titolare dei diritti e che l'accesso alle fonti avvenga in modo legittimo;
- l'introduzione di nuove fattispecie penali legate all'uso dell'IA e a tutela della proprietà intellettuale.

Poiché la Legge italiana sull'IA è stata elaborata prima dell'adozione dell'AI Act, sarà necessario attendere i decreti delegati per comprenderne appieno l'impatto e il grado di integrazione con il quadro europeo. Al momento, infatti, emergono profili di continuità, ma anche di potenziale incertezza interpretativa.

Per qualsiasi questione relativa ai temi discussi in questa nota, potete contattare qualsiasi avvocato del nostro studio con cui siete abitualmente in contatto o gli autori di seguito.

MILANO

Roberto Bonsignore
+39 02 7260 8230
rbonsignore@cgsh.com

Giulia Checcacci
+39 02 7260 8224
gcheccacci@cgsh.com

Giulia De Bosio
+39 02 7260 8292
gdebosio@cgsh.com

ROMA

Giuseppe Scassellati-Sforzolini
+39 06 6952 2220
gscassellati@cgsh.com

Federica Mammì Borruto
T: +39 06 6952 2826
fmammiborruto@cgsh.com

Paola Maria Onorato
T: +39 06 6952 2654
ponorato@cgsh.com

© Cleary Gottlieb Steen & Hamilton LLP, 2025. Tutti i diritti sono riservati.
Questo memorandum, che contiene informazioni generali e non può essere considerato come parere legale, è destinato ai clienti e amici di Cleary Gottlieb al fine di aggiornarli su sviluppi normativi che potrebbero essere di loro interesse. Attraverso questo memorandum "Cleary Gottlieb" e lo "studio" si riferiscono a Cleary Gottlieb Steen & Hamilton LLP e ad entità ad esso collegate in alcune giurisdizioni; il termine "uffici" comprende le sedi di tali entità collegate.

1. Il modello italiano di *governance* dell'IA: criteri operativi concreti, incertezze interpretative e ampie deleghe

La Legge italiana sull'IA introduce una disciplina destinata inevitabilmente a interagire con la normativa europea ed in particolare con l'AI Act, il quale, nel disciplinare il settore dell'IA, adotta un approccio *risk-based*, distinguendo i sistemi di IA in base al rischio ad essi associato e dettando una disciplina progressivamente più rigorosa.

La normativa italiana dovrebbe costituire una cornice complementare rispetto a quella sovranazionale e colmare gli spazi lasciati alla discrezionalità degli Stati membri.

Coerentemente, quindi, il Legislatore afferma che la Legge italiana sull'IA:

- va interpretata e applicata conformemente all'AI Act (articolo 1, comma 2);
- non prevede nuovi obblighi oltre quelli già previsti dall'AI Act (articolo 3, comma 5).

Tuttavia, diverse norme della Legge italiana sull'IA sono già pienamente applicabili, mentre, come noto, l'AI Act prevede un meccanismo di attuazione progressiva, in base al quale solo una parte degli obblighi dettati dallo stesso sono oggi vincolanti per gli operatori del settore.

Ne consegue la necessità di prestare particolare attenzione alla Legge italiana sull'IA, che impone obblighi di immediata efficacia e le cui disposizioni presentano sin d'ora diversi profili di incertezza applicativa, sollevando al contempo dubbi circa la loro compatibilità con il quadro normativo europeo.

1.1 Deleghe e attuazione dell'AI Act: una disciplina in via di definizione

L'AI Act, sebbene direttamente applicabile, troverà concreta attuazione anche attraverso la Legge italiana sull'IA, la quale delega al Governo l'adozione di uno o più decreti legislativi volti a definire gli aspetti cruciali per il settore.

In base all'articolo 16, il Governo dovrà delineare il regime giuridico relativo alle attività di addestramento dei sistemi di intelligenza artificiale, definendo i diritti e gli obblighi dei soggetti che esercitano tale attività, nonché predisponendo strumenti di tutela, anche di natura inibitoria, e un adeguato apparato sanzionatorio.

Inoltre, ai sensi dell'articolo 24, il Governo sarà chiamato a intervenire in modo trasversale sull'ordinamento per adeguare la normativa nazionale all'AI Act e per ridefinire la disciplina in diversi settori.

Oltre agli interventi finalizzati a preparare il tessuto socioeconomico del Paese all'avvento di questo tipo di tecnologia, come ad esempio la promozione di percorsi di alfabetizzazione e formazione in materia di IA, il Governo dovrà intervenire sull'ecosistema normativo sia sotto il profilo sostanziale che processuale.

In particolare, oltre agli interventi in materia penale di cui si dirà di seguito, i decreti delegati dovranno definire l'applicazione delle regole della responsabilità civile al settore dell'IA, disciplinando i casi di realizzazione e impiego illeciti dei sistemi di IA. In tale contesto, il Governo dovrà prevedere strumenti, cautelari e/o sanzionatori, idonei a prevenire la diffusione di contenuti generati illecitamente con sistemi di intelligenza artificiale e disciplinare la loro rimozione.

L'intervento in materia di responsabilità civile potrebbe introdurre novità di grande rilievo. Al momento, è possibile ipotizzare soltanto alcuni scenari, tra cui l'adozione di regimi di responsabilità oggettiva e responsabilità solidale, nonché obblighi assicurativi per sviluppatori e/o utilizzatori di sistemi di IA. E' comunque certo che, per garantire un'effettiva tutela dei cittadini, il Governo dovrà intervenire non solo sul piano rimediale, ma, ai sensi dell'art. 24, comma 5, lett. d), anche sulle procedure azionabili e sui meccanismi probatori propri del processo civile, tenendo in considerazione l'asimmetria informativa che spesso si viene a creare tra il soggetto leso e il fornitore, sviluppatore o utilizzatore dei sistemi di IA più avanzati.

Al Governo sono concessi dodici mesi di tempo per l'attuazione delle deleghe appena menzionate. Tuttavia, la Legge italiana sull'IA prevede che alcune misure dovranno essere adottate in tempi più brevi. Ad esempio:

- il Ministro della Salute avrà 120 giorni per disciplinare il trattamento semplificato dei dati

personali per ricerca e sperimentazione anche tramite sistemi di IA e *machine learning* (articolo 9);

- il Ministero del Lavoro avrà 90 giorni per istituire l'Osservatorio sull'adozione dell'IA nel mondo del lavoro (articolo 12).

Inoltre, pur senza un termine specifico, è previsto che AGENAS (l'Agenzia Nazionale per i servizi sanitari Regionali) potrà emanare linee guida per l'anonimizzazione e la generazione di dati sintetici in ambito sanitario (art. 8).

1.2 Autorità nazionali per l'intelligenza artificiale

Come anticipato, la Legge italiana sull'IA individua le autorità competenti per la vigilanza e il controllo sull'attuazione della normativa nazionale e dell'AI Act, nonché, più in generale, sull'intero settore dell'IA.

L'articolo 20 designa l'Agenzia per l'Italia Digitale ("***AgID***") e l'Agenzia per la Cybersicurezza Nazionale ("***ACN***") quali Autorità nazionali per l'intelligenza artificiale, lasciando impregiudicato il ruolo di Banca d'Italia, CONSOB e IVASS come autorità di vigilanza dei mercati bancari, finanziari e assicurativi (AI Act, articolo 74, paragrafo 6). In particolare, viene chiarito che l'AgID assumerà funzioni di promozione dello sviluppo dell'IA, oltre a compiti di notifica, valutazione, accreditamento e monitoraggio degli organismi di valutazione della conformità, mentre l'ACN sarà responsabile della vigilanza sui sistemi di IA, con poteri ispettivi e sanzionatori, e fungerà da autorità di vigilanza del mercato e punto di contatto unico con le istituzioni UE. Anche in questo ambito i decreti delegati avranno un ruolo fondamentale perché dovranno attribuire a queste autorità gli specifici poteri sanzionatori previsti, tra l'altro, anche dall'AI Act.

Tale designazione da parte del Legislatore italiano ha suscitato perplessità fin dalla pubblicazione del disegno di legge. La scelta di due agenzie di matrice governativa – anziché di autorità amministrative indipendenti – è stata infatti ritenuta da molti non idonea ad assicurare un adeguato livello di indipendenza. Peraltro, tale timore era stato già avanzato dalla Commissione Europea nel parere C(2024)7814 (il "***Parere***"), col quale aveva sottolineato la necessità che le autorità nazionali competenti per la sorveglianza sull'implementazione dell'AI Act godano di piena indipendenza funzionale e operativa, come previsto, ad esempio, per altre autorità quali il Garante per la protezione dei dati personali ("***Garante Privacy***").

1.3 Stimoli agli operatori del settore e criteri per la collaborazione tra pubblico e privato

Sebbene la sua reale portata potrà essere realmente apprezzata solo dopo l'adozione dei decreti delegati, la Legge italiana sull'IA riconosce chiaramente la rilevanza strategica dello sviluppo e dell'utilizzo dell'IA per il Paese. Infatti, l'art. 5 qualifica l'IA come motore di crescita economica e competitività nazionale, sottolineando l'importanza della creazione di un mercato equo e concorrenziale attorno a questa tecnologia.

In quest'ottica, la Legge italiana sull'IA istituisce strumenti a supporto dell'ecosistema imprenditoriale e della collaborazione pubblico-privato nell'implementazione di soluzioni di IA.

In *primis*, l'articolo 19 prevede che la Presidenza del Consiglio elabori una Strategia Nazionale per l'Intelligenza Artificiale, da aggiornare e approvare almeno biennalmente, con l'obiettivo di promuovere *partnership* strategiche pubblico-privato e programmi di ricerca finanziati dallo Stato. La sua attuazione sarà coordinata da un Comitato di coordinamento *ad hoc*, presieduto dal Presidente del Consiglio.

L'articolo 5 stabilisce inoltre alcuni criteri che, ferma restando la necessità di un'applicazione conforme al diritto dell'UE[1], orienteranno la scelta dei fornitori di sistemi e di modelli di IA da parte delle piattaforme di *e-procurement* delle PA. In particolare, queste dovranno privilegiare fornitori che garantiscano:

- localizzazione ed elaborazione dei dati strategici in *data center* posti nel territorio nazionale;

[1] Si pensi in particolare al divieto di restrizioni alle libertà di stabilimento e di prestazione di servizi all'interno della UE in base alla nazionalità o alla residenza (salvo che siano dettate da motivi di ordine pubblico o di pubblica sicurezza).

- procedure di *disaster recovery* e *business continuity* attuate in *data center* posti sul territorio nazionale;
- elevati standard di sicurezza e trasparenza nell'addestramento e nello sviluppo di applicazioni di IA generativa.

Infine, la Legge italiana sull'IA autorizza investimenti fino a un miliardo di euro, da effettuarsi in conformità alla già menzionata Strategia Nazionale per l'Intelligenza Artificiale, per sostenere le imprese italiane operanti nel settore dell'IA, della cybersicurezza e delle tecnologie strumentali (incluse 5G, *mobile edge computing*, *Web 3*). In particolare, gli investimenti verranno effettuati sotto forma di *equity* e *quasi-equity* nel capitale di rischio di:

- PMI innovative ad alto potenziale di sviluppo aventi sede operativa in Italia, con particolare focus sul *seed financing, start up financing, early-stage financing* e *scale-up financing*;
- altre imprese con elevato potenziale di sviluppo e altamente innovative per promuovere lo sviluppo di campioni tecnologici nazionali.

2. Principi fondativi: centralità dell'essere umano e protezione dei dati

La Legge italiana sull'IA contiene in apertura una serie di principi generali che delineano la cornice di riferimento per l'intero sistema, ponendo al centro il rispetto dei diritti fondamentali e delle libertà costituzionali. Fatto salvo il settore della sicurezza e della difesa nazionale, per il quale dovranno essere adottate specifiche linee guida, la legge rafforza l'impostazione europea, sottolineando la necessità di prevenire usi distorsivi della tecnologia.

L'articolo 3, in particolare, afferma che la ricerca, la sperimentazione, lo sviluppo e l'impiego di sistemi di IA devono avvenire nel rispetto della dignità umana, della protezione dei dati personali, della trasparenza e della non discriminazione, e soprattutto nel rispetto dell'autonomia e del potere decisionale della persona. Quest'ultimo principio rappresenta il fulcro della normativa: la legge, in linea con l'approccio antropocentrico dell'AI Act, introduce un principio generale di non delegabilità della decisione, sancendo che nessun processo automatizzato possa sostituire integralmente la volontà umana.

L'art. 4 disciplina, invece, i principi in materia di informazione e protezione dei dati personali, vietando che i sistemi di IA compromettano la libertà, il pluralismo o l'imparzialità dell'informazione. Il trattamento dei dati deve rispettare i criteri di liceità, correttezza e trasparenza previsti dal Regolamento (UE) 2016/679 ("***GDPR***") e i sistemi di IA dovranno essere progettati in conformità con tali requisiti.

È inoltre previsto un obbligo di trasparenza rafforzato per i soggetti che impiegano sistemi di IA nell'erogazione di servizi. L'articolo 4 stabilisce che le informative sul trattamento dei dati connessi all'utilizzo di sistemi di IA devono essere rese con linguaggio chiaro e semplice, consentendo agli utenti di comprendere i rischi ed eventualmente di opporsi al trattamento. Ciò richiede una valutazione e un eventuale adeguamento delle informative esistenti ai nuovi standard di trasparenza.

Infine, un'attenzione specifica è dedicata alla tutela dei minori per i quali sono previste tutele rafforzate rispetto a quelle del GDPR: per i soggetti di età inferiore a 14 anni l'accesso ai sistemi di IA e il relativo trattamento dei dati richiedono il consenso dei genitori, mentre i minori tra 14 e 18 anni possono esprimerlo autonomamente, a condizione che le informazioni relative al trattamento dei dati siano agevolmente accessibili e comprensibili.

Restano, tuttavia, senza risposta diversi aspetti rilevanti in tema di raccolta e utilizzo dei dati in materia di IA, quale, ad esempio l'applicazione del diritto all'oblio sancito dal GDPR.

3. L'introduzione di una disciplina settoriale

Andando oltre al quadro normativo stabilito dall'AI Act, la Legge italiana sull'IA interviene in alcuni settori specifici dettando una disciplina dei sistemi di IA che prescinde dal rischio a loro associato. La normativa individua alcuni ambiti, tra cui sanità, pubblica amministrazione, giustizia e lavoro, e per questi introduce prescrizioni particolari, orientate a rafforzare la supervisione umana e la responsabilità degli operatori. Al riguardo tuttavia, già nel Parere, la Commissione Europea aveva avvertito circa il rischio di introdurre restrizioni non necessarie per i sistemi di IA non classificati ad alto rischio, sottolineando che tale approccio potrebbe contribuire alla

frammentazione del mercato unico europeo in materia di IA.

3.1 Sanità e ricerca scientifica

In ambito sanitario, l'articolo 7 consente l'impiego dell'IA per finalità di prevenzione, diagnosi e cura, precisando tuttavia che la responsabilità della decisione terapeutica resta in capo al medico. Questa disposizione, in linea con l'approccio antropocentrico della legge, riafferma il principio di responsabilità personale del professionista e impedisce che l'automazione algoritmica sostituisca il giudizio clinico, ponendo una chiara barriera contro il rischio di automatizzazione delle decisioni mediche.

In tale ambito, il legislatore italiano ha, inoltre, deciso di adottare tutele maggiori rispetto a quanto previsto dall'AI Act, imponendo standard di trasparenza più rigorosi. Mentre quest'ultimo richiede trasparenza sull'impiego di sistemi automatizzati, ma non impone un obbligo di illustrare ai pazienti le logiche interne del modello né di giustificare i benefici attesi, l'Italia ha deciso di prevedere obblighi informativi in ambito sanitario più ampi e rigorosi, prevedendo, oltre alla comunicazione dell'impiego di sistemi di IA, anche la descrizione dei vantaggi diagnostici e terapeutici e la logica decisionale sottostante.

Il legislatore interviene anche in materia di ricerca scientifica in ambito sanitario, introducendo rilevanti novità rispetto alla disciplina dettata dal D. Lgs. n. 196/2003 ("***Codice Privacy***").

Riconoscendo il rilevante interesse pubblico del trattamento dei dati personali effettuato da enti pubblici e privati senza scopo di lucro per finalità di ricerca e sperimentazione di sistemi di IA a fini medici, si prevede l'esclusione della necessità del consenso al trattamento per tali soggetti. Per gli stessi fini e ai medesimi soggetti viene inoltre permesso l'uso secondario (ossia il trattamento per scopi diversi da quelli per cui i dati sono stati inizialmente raccolti) dei dati, previa semplice informativa, purché i dati non contengano elementi identificativi diretti, salvi i casi in cui la conoscenza dell'identità degli interessati non possa essere evitata senza pregiudicare l'obiettivo principale di questa disposizione, ossia la tutela della loro salute.

È previsto, però, un regime sostanzialmente autorizzatorio del Garante Privacy, che dovrà essere informato almeno 30 giorni prima dell'avvio del trattamento o del riutilizzo dei dati e potrà intervenire con un provvedimento di blocco.

In ultimo, l'articolo 8 autorizza, previa informativa all'interessato, il trattamento di dati personali per finalità di anonimizzazione, pseudonimizzazione o sintetizzazione se eseguito per fini legati allo sviluppo di sistemi di IA finalizzati all'assistenza sanitaria.

Stante la rilevanza delle novità apportate, non vi è dubbio che le previsioni in tema di trattamento dei dati personali dovranno essere lette unitamente alle norme già in vigore da tempo.

3.2 Pubblica Amministrazione

Un altro settore strategico oggetto di disciplina specifica è quello della pubblica amministrazione. La Legge italiana sull'IA prevede che l'adozione di sistemi di IA da parte delle amministrazioni pubbliche sia finalizzata esclusivamente a funzioni di supporto decisionale, organizzazione e semplificazione, senza mai sostituire la responsabilità dell'organo o del funzionario competente. Questa impostazione riflette l'esigenza di assicurare *accountability* istituzionale, evitando che processi automatizzati possano determinare decisioni con effetti diretti sui diritti dei cittadini.

In linea con le esigenze di trasparenza che caratterizzano l'esercizio del potere amministrativo e dell'impostazione antropocentrica, sulla pubblica amministrazione graverà l'obbligo sancito dall'articolo 14, comma 2, secondo cui dovranno essere assicurate ai soggetti interessati la "*conoscibilità*" e la "*tracciabilità*" del funzionamento e dell'utilizzo dei sistemi di IA impiegati nelle proprie attività.

3.3 Lavoro

Gli articoli 12 e 13 limitano l'impiego dei sistemi di IA nelle professioni intellettuali e, più in generale, nelle attività lavorative, sottolineando la necessità che l'utilizzo delle tecnologie non si traduca in una sostituzione della prestazione umana tale da compromettere la dignità e la sicurezza del lavoratore.

4. Il diritto d'autore nell'era dell'IA: principi generali e *text and data mining*

La nuova Legge italiana sull'IA introduce rilevanti novità in materia di diritto d'autore, con l'obiettivo di adeguare la storica legge n. 633/1941 ("***Legge sul Diritto d'Autore***") alle sfide poste dalle tecnologie digitali emergenti.

L'intervento legislativo si articola lungo tre direttrici principali: (*i*) ribadire la centralità del fattore umano nelle opere realizzate con l'ausilio di strumenti di IA; (*ii*) favorire lo sviluppo tecnologico mediante l'estensione delle eccezioni di *text and data mining* ("***TDM***") ai sistemi di IA (purché nel rispetto del c.d. *opt-out*); (*iii*) rafforzare il quadro sanzionatorio attraverso la previsione di nuove fattispecie penali per violazioni in ambito TDM (cfr. *infra* par. 5).

In particolare, la Legge italiana sull'IA:

- modifica l'articolo 1, chiarendo che le opere assistite da IA possono beneficiare della tutela autorale solo se risultano da un apporto intellettuale umano sostanziale;
- introduce l'articolo 70-*septies*, che estende l'eccezione TDM alle riproduzioni ed estrazioni effettuate tramite modelli e sistemi di IA, inclusa l'IA generativa;
- modifica l'articolo 171, inserendo al comma 1 la nuova lettera *a-ter*, che prevede sanzioni penali per le violazioni delle norme TDM anche quando poste in essere tramite IA (cfr. *infra* par. 5).

4.1 Opere assistite da IA

L'intervento normativo consolida in via definitiva una visione antropocentrica della creatività: la tutela del diritto d'autore spetta esclusivamente alle opere dell'ingegno umano. La protezione potrà estendersi alle opere create con strumenti di IA esclusivamente laddove l'autore umano abbia apportato un contributo creativo sostanziale.

Questa scelta normativa è coerente con la giurisprudenza italiana ed europea sull'originalità e paternità dell'opera, gli orientamenti statunitensi, nonché i principi fondativi della Convenzione di Berna (1886), che collega la protezione autoriale all'opera dell'ingegno quale espressione della personalità dell'autore.

4.2 Text and Data Mining (TDM)

Accanto al tema della proteggibilità delle opere assiste da IA, la Legge italiana sull'IA introduce l'articolo 70-*septies*, il quale disciplina espressamente le attività di TDM condotte mediante modelli e sistemi di intelligenza artificiale, inclusi quelli generativi.

La norma consente la riproduzione ed estrazione di testi o dati da opere o materiali ai quali il soggetto abbia legittimamente accesso, disponibili *online* o in banche dati, attraverso modelli e sistemi di IA, anche generativa, purché nel rispetto delle previsioni degli articoli 70-*ter* e 70-*quater* (introdotti con il d.lgs. n. 177/2021 in attuazione della Direttiva (UE) 2019/790, nota come Direttiva Copyright DSM). In particolare, il 70-*ter* autorizza attività di TDM quando effettuate da organismi di ricerca o istituti di tutela del patrimonio culturale per scopi scientifici, mentre il 70-*quater* consente attività di TDM per qualsiasi scopo, anche commerciale, a condizione che l'utilizzo delle opere non sia stato espressamente riservato dal titolare dei diritti (c.d. *opt-out*).

5. Le disposizioni penali in materia di IA

La Legge italiana sull'IA introduce anche importanti novità in ambito penale, con l'obiettivo di rafforzare la risposta dell'ordinamento alle nuove minacce generate dalle tecnologie digitali. L'intervento del legislatore si articola lungo due direttrici principali: da un lato, l'introduzione di nuove fattispecie di reato; dall'altro, la previsione di circostanze aggravanti legate all'impiego dell'IA.

In particolare, la Legge italiana sull'IA:

- introduce il nuovo reato di "*Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale*" (art. 612-*quater* c.p.), che punisce con la reclusione da uno a cinque anni chiunque cagioni un danno ingiusto ad una persona cedendo, pubblicando o diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di IA e idonei a indurre in inganno sulla loro genuinità. Tale disposizione è finalizzata a contrastare l'ormai dilagante fenomeno dei cosiddetti deepfake, spesso lesivi della reputazione e della

libertà morale altrui. Il nuovo delitto è punibile a querela della persona offesa, ma diventa procedibile d'ufficio se il fatto è connesso con un altro delitto procedibile d'ufficio, o se commesso nei confronti di persona incapace o di una pubblica autorità a causa delle funzioni esercitate;

- integra la disciplina del diritto d'autore, modificando l'art. 171, primo comma, della Legge sul Diritto d'Autore con la nuova lettera a-*ter*. La norma sanziona la riproduzione o l'estrazione di testi o dati da opere o materiali disponibili *online* o in banche dati in violazione degli articoli 70-*ter* e 70-*quater*, anche quando effettuata tramite sistemi di IA. L'obiettivo è contrastare pratiche scorrette di *scraping* e *text/data mining* non autorizzato (ad esempio, nel caso di *scraping* di materiali per i quali il titolare dei diritti abbia esercitato l'*opt-out*);
- prevede un'ulteriore modifica ai reati in materia di diritto d'autore estendendo la nozione di "*opere dell'ingegno*" di cui all'art. 1 della Legge sul Diritto d'Autore, che include adesso anche le opere realizzate con l'ausilio dell'IA. Ciò comporta, conseguentemente, l'estensione dell'ambito applicativo del reato di cui all'art. 171-*ter*, che punisce chi, a fini di lucro o per uso personale, duplica, riproduce, trasmette o diffonde pubblicamente un'opera in violazione del diritto d'autore;
- inserisce una nuova circostanza aggravante ad effetto comune (art. 61, n. 11-*undecies*, c.p.)[2], applicabile dunque a tutte le fattispecie di reato, che prevede un aumento della pena fino a un terzo nei casi in cui l'impiego di sistemi di IA abbia costituito un mezzo insidioso, ostacolato la pubblica o privata difesa o aggravato le conseguenze del reato;
- modifica altre fattispecie di reato introducendo circostanze aggravanti speciali concernenti l'impiego dell'IA, e nello specifico *(i)* il delitto di attentati contro i diritti politici del cittadino (art. 294 c.p.), la cui pena risulta adesso aumentata se l'inganno che impedisce in tutto o in parte l'esercizio di un diritto politico è realizzato tramite l'impiego di IA; e *(ii)* i reati di aggiotaggio (art. 2637 c.c.) e manipolazione del mercato (art. 185, D.Lgs. 58/1998), per i quali è previsto un aumento di pena qualora il fatto sia commesso mediante l'impiego di sistemi di IA.

6. IA e responsabilità degli enti *ex* D. Lgs. 231/2001

La Legge italiana sull'IA non interviene direttamente sul regime della responsabilità amministrativa degli enti previsto dal D. Lgs. 231/2001 ("***Decreto 231***"). Tuttavia, le novità previste in ambito penale produrranno effetti, seppur indiretti, sulla responsabilità delle persone giuridiche e, in particolare, sull'aggiornamento dei modelli organizzativi.

In particolare, sebbene la previsione di un aggravante comune (art. 61, n. 11-*decies*, c.p.) per i reati commessi mediante IA si applichi soltanto alle persone fisiche autrici del reato presupposto, la circostanza che l'IA possa agevolare la commissione di illeciti impone una riflessione anche sul piano della prevenzione aziendale, potendosi riflettere non solo in una maggiore esposizione al rischio, ma anche in una valutazione più severa delle condotte ai fini della quantificazione della sanzione per l'ente.

Ulteriori novità derivano anche dalla già menzionata estensione della definizione di "*opere dell'ingegno*" contenuta nell'art. 1 della Legge sul Diritto d'Autore, che ora comprende anche le opere realizzate con l'ausilio dell'IA. Poiché l'art. 25-*novies* del Decreto 231 include tra i reati presupposto tutte le violazioni dell'art. 171-*ter* della Legge sul Diritto d'Autore, ne consegue che anche le condotte illecite riferibili a tali "nuove" opere ricadono oggi nel perimetro della responsabilità degli enti. Le imprese potranno quindi essere chiamate a rispondere quando tali violazioni – come la duplicazione, la diffusione o la riproduzione abusiva a fini di lucro – siano poste in essere da un dipendente o da un soggetto in posizione apicale a vantaggio o nell'interesse dell'ente. In questi casi, le società potranno essere soggette a una sanzione pecuniaria fino a cinquecento quote (pari a un

[2] Si segnala che la disposizione era stata originariamente inserita come comma 11-*decies* dell'art. 61 c.p., duplicando una numerazione già esistente. La numerazione è stata successivamente rettificata con comunicato pubblicato nella Gazzetta Ufficiale n. 242 del 17 ottobre 2025.

massimo di 774.685 euro) e, nei casi più gravi, anche alle sanzioni interdittive previste dal Decreto 231 (tra cui l'interdizione dall'esercizio dell'attività; la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; il divieto di contrattare con la pubblica amministrazione; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi) per una durata massima di un anno.

Non sono stati inclusi invece tra i reati presupposto della responsabilità degli enti le nuove fattispecie, introdotte dalla Legge italiana sull'IA, di "Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale" (art. 612-*quater* c.p.) e di riproduzione o estrazione illecita di dati tutelati dal diritto d'autore tramite IA (art. 171, primo comma, lett. a-*ter* della Legge sul Diritto d'Autore).

Alla luce di tali sviluppi, occorrerà dunque valutare la necessità di aggiornare i propri modelli organizzativi e protocolli interni, sia sotto un profilo formale (per recepire le nuove circostanze aggravanti e le altre novità rilevanti), sia da quello sostanziale. In particolare, potrebbe essere necessario modificare la mappatura delle attività a rischio per includere i nuovi scenari legati all'uso dell'IA nei processi aziendali, nonché rafforzare i controlli interni e le misure di prevenzione.

È probabile che una società già pienamente conforme al Decreto 231 disponga di controlli, concepiti per altre fattispecie di reato, che possano risultare efficaci anche rispetto alle nuove condotte (si pensi a quelli in materia di violazione del diritto d'autore), ma sarà comunque opportuno valutare l'introduzione di ulteriori presidi di controllo, capaci di intercettare anche i rischi derivanti dall'utilizzo – intenzionale o non controllato – di sistemi di IA. Tra questi, protocolli e procedure che assicurino la tracciabilità, la responsabilità e il controllo delle decisioni che coinvolgano tecnologie di IA.

7. La delega al Governo in materia penale

Il quadro delle misure penali connesse all'uso dell'IA è ancora in via di definizione e non si esaurirà in quanto finora illustrato. Il legislatore ha infatti conferito al Governo un'ampia delega ad intervenire in materia di diritto penale sostanziale e processuale, nonché in tema di responsabilità degli enti.

In particolare, il Governo è chiamato a:

- 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'intelligenza artificiale, qualora tale omissione comporti un pericolo concreto per la vita, la sicurezza individuale o collettiva o per la sicurezza dello Stato;
- precisare i criteri di imputazione della responsabilità penale delle persone fisiche e degli enti per illeciti inerenti a sistemi di IA, tenendo conto del livello effettivo di controllo esercitato sui sistemi di IA;
- regolare l'utilizzo dei sistemi di IA nelle indagini preliminari;
- modificare la normativa sostanziale e processuale vigente a fini di coordinamento e di razionalizzazione del sistema.

Sarà dunque interessante osservare come verrà attuata questa ampia delega, soprattutto in relazione ai nuovi reati che potrebbero essere introdotti e che potrebbero ampliare il catalogo delle fattispecie rilevanti ai fini del Decreto 231.

In un contesto normativo in cui tecnologia, *compliance* e diritto penale tendono a intrecciarsi sempre più, gli operatori economici sono chiamati a integrare la governance dell'IA nei modelli organizzativi e nei sistemi di gestione del rischio, adeguandosi tanto sul piano tecnico quanto su quello giuridico.

8. Conclusioni

La Legge italiana sull'IA rappresenta un intervento normativo di portata significativa, il cui reale impatto potrà però essere valutato compiutamente solo al termine della futura fase attuativa. Il Legislatore ha, infatti, conferito al Governo un mandato ampio attraverso le deleghe previste dagli articoli 16 e 24, che dovranno tradursi in decreti legislativi entro dodici mesi dall'entrata in vigore della Legge italiana sull'IA. È da questi provvedimenti attuativi che dipenderà l'effettiva capacità della nuova disciplina italiana di incidere concretamente sulle modalità di

sviluppo e utilizzo dell'IA, senza però interferire con l'applicazione uniforme dell'AI Act. Anche in considerazione della rapida evoluzione tecnologica, queste innovazioni normative dovranno essere attentamente e prontamente valutate attraverso un monitoraggio costante.

…

CLEARY GOTTLIEB