

Camera dei Deputati
Commissioni riunite Affari costituzionali e Giustizia

Dlgs di adeguamento della normativa nazionale alle disposizioni dell'AI Act in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale - Criticità e raccomandazioni

1. Premessa

Meta condivide pienamente l'obiettivo perseguito dal decreto in oggetto volto a garantire un'attuazione efficace delle disposizioni dell'AI Act e a introdurre sanzioni effettive, proporzionate e dissuasive per le relative violazioni. Fatta salva ogni valutazione in merito alla qualificazione di Meta come fornitore, deployer o utilizzatore finale di sistemi di IA ad alto rischio ai sensi dell'AI Act, e in considerazione dell'impegno dell'azienda nei confronti dell'ecosistema dell'innovazione italiano e del mercato unico digitale europeo più in generale, Meta è consapevole della rilevanza di tali obiettivi ai fini della tutela dei cittadini e del rafforzamento della fiducia nell'innovazione tecnologica.

Nell'esaminare il testo, ci permettiamo tuttavia di segnalare alcune criticità che sottoponiamo all'attenzione del Parlamento, auspicando che possano essere considerate nel corso dell'iter parlamentare. Tali criticità attengono in particolare alla formulazione della nuova fattispecie penale di cui all'articolo 437-bis, al regime di responsabilità civile e alla struttura complessiva delle garanzie riconosciute agli operatori conformi al regolamento (UE) 2024/1689.

Il decreto introduce pene detentive fino a dieci anni per *“chiunque omette di adottare le misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato o l'utilizzo professionale di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi”*. Al riguardo, riteniamo che, tenuto conto del fatto che l'applicazione delle corrispondenti disposizioni dell'AI Act è stata prorogata al 2 dicembre 2027 e che non sono state ancora elaborate né linee guida né codici di condotta ai sensi dell'articolo 95 del Regolamento, l'articolo 437-bis non sia in grado di soddisfare il mandato di cui al Considerando 168 dell'AI Act, che richiede l'introduzione di sanzioni *“effettive, proporzionate e dissuasive [...] tenendo conto della natura, della gravità e della durata della violazione.”*

Tale regime di responsabilità penale non trova alcun fondamento nell'AI Act e si pone altresì in contrasto con lo spirito stesso del Regolamento, che calibra il proprio apparato sanzionatorio esclusivamente intorno a sanzioni amministrative pecuniarie.

Si rileva inoltre che l'articolo 437-bis si pone in tensione con i principi di tassatività e personalità della responsabilità penale sanciti dagli articoli 25 e 27 della Costituzione, nonché con i principi di legalità e di giusto processo di cui agli articoli 6 e 7 CEDU, e va significativamente oltre quanto previsto sia dall'AI Act che da quanto adottato da qualsiasi altro Stato Membro dell'Unione europea in sede di attuazione.

L'AI Act definisce un'architettura sanzionatoria completa e autosufficiente. Al riguardo, si rileva che in nessun punto il Regolamento richiama, contempla o indirizza gli Stati Membri verso sanzioni di natura penale. Va inoltre considerato che le negoziazioni relative al Regolamento hanno avuto una durata di tre anni (2021-2024), con un ampio e approfondito dibattito sull'intensità del regime sanzionatorio, e il testo finale riflette una scelta consapevole e meditata.

Tale scelta riposa su ragioni strutturali:

1. l'approccio graduato del Regolamento - che differenzia obblighi e responsabilità in funzione del rischio e del ruolo dell'operatore - si accompagna a una struttura sanzionatoria amministrativa anch'essa graduata: la responsabilità penale, con il suo schema binario colpevole/non colpevole, non è compatibile con questa architettura differenziata;
2. il Considerando 1 afferma che il Regolamento mira a promuovere l'adozione di un'intelligenza artificiale "antropocentrica e affidabile", garantendo nel contempo un livello elevato di protezione: le sanzioni amministrative assolvono alla funzione deterrente senza produrre l'effetto di disincentivo all'innovazione che l'esposizione penale inevitabilmente comporta per i soggetti chiamati ad adottare decisioni aziendali;
3. l'AI Act è un regolamento direttamente applicabile, adottato proprio al fine di conseguire regole uniformi nel mercato interno: qualora gli Stati Membri vi sovrappongano regimi penali divergenti, la frammentazione che il Regolamento era destinato a prevenire riemerge in diretta contraddizione con i suoi obiettivi.

Le conseguenze di tale impostazione rischiano di essere profonde, per l'Italia e per l'Unione europea nel suo complesso. Qualora ingegneri e responsabili della conformità (*compliance*) siano esposti a pene detentive per condotte in relazione alle quali non esistono standard giuridicamente certi, le aziende potrebbero essere indotte a limitare eccessivamente le funzionalità dei propri sistemi per il mercato italiano. In termini ancora più paradossali, un operatore pienamente conforme ai requisiti dell'AI Act in 26 Stati Membri potrebbe essere sottoposto a procedimento penale in Italia per la medesima condotta: questa è l'opposto dell'armonizzazione che il Regolamento persegue.

Il quadro amministrativo dell'AI Act fornisce indicazioni chiare su cosa costituisca una violazione e su come essa debba essere sanzionata. L'introduzione della responsabilità penale aggiunge discrezionalità nell'esercizio dell'azione penale, interpretazione giudiziale ed esposizione personale che non possono essere ricondotte alle categorie di conformità definite dal Regolamento.

Auspichiamo pertanto che il Parlamento possa considerare una revisione di alcune disposizioni, come di seguito illustrate, al fine di dotare il Paese di un quadro normativo che possa conciliare - a nostro avviso - elevati standard di sicurezza e, assieme, certezza giuridica per gli operatori del settore.

2. Principale criticità

Lo schema di decreto legislativo introduce due nuovi meccanismi di responsabilità applicabili a qualsiasi soggetto coinvolto nella catena del valore dei sistemi di IA ad alto rischio:

1. Responsabilità penale (Art. 437-bis)

La disposizione configura una nuova fattispecie di reato a carico di chiunque sia coinvolto nelle fasi di progettazione, addestramento, produzione, immissione sul mercato o utilizzo professionale di un sistema di IA ad alto rischio, ometta di adottare misure tecniche di sicurezza idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi, o ometta misure di sorveglianza umana ovvero chiunque alteri il sistema stesso.

La pena - da tre a dieci anni di reclusione - si applica al verificarsi di un pericolo concreto per la vita o l'incolumità delle persone, prescindendo dall'effettivo verificarsi di un danno.

2. Responsabilità civile (Artt. 18-23)

Il regime civilistico introduce tre elementi chiave:

- a. L'inversione dell'onere della prova a favore dei ricorrenti nelle azioni di responsabilità civile in caso di violazione dell'AI Act;
- b. La facoltà riconosciuta ai tribunali di disporre, su istanza della parte che allega di avere subito il danno, la divulgazione della documentazione tecnica nelle cause di responsabilità civile;
- c. La previsione espressa per cui la piena conformità all'AI Act, anche in presenza di certificazione, non esclude di per sé la responsabilità del convenuto, nell'ambito delle azioni civili.

3. Principio di legalità e diritti alla difesa e al giusto processo

3.1 Indeterminatezza della fattispecie

La fattispecie penale di cui all'articolo 437-bis richiede ai giudici di determinare, ex post, se le misure tecniche adottate da uno sviluppatore fossero "misure tecniche idonee a prevenire malfunzionamenti". Il decreto non fornisce tuttavia alcun parametro oggettivo per tale valutazione: nessun riferimento a standard armonizzati, nessuna previsione di "safe harbour", nessun criterio tecnico di riferimento. Ne consegue che **singoli giudici - esperti di diritto, ma non necessariamente esperti tecnici di IA - saranno chiamati a pronunciarsi autonomamente sull'adeguatezza delle misure di sicurezza dell'IA, determinando un**

rischio concreto di decisioni divergenti sulla medesima tecnologia e, nella peggiore delle ipotesi, di pronunce prive di adeguato fondamento tecnico. Tale incertezza lede il diritto di difesa e al giusto processo degli sviluppatori e genera incertezza e imprevedibilità giuridica per tutti gli operatori del settore, per gli investitori e, in ultima analisi, per i cittadini che beneficiano delle applicazioni dell'IA.

Il decreto solleva pertanto profili di illegittimità costituzionale con riguardo al principio della certezza del diritto, sancito dall'articolo 25 della Costituzione italiana nonché dall'articolo 7 della CEDU. Tale principio impone che le norme penali siano formulate con sufficiente precisione così da consentire agli individui di prevedere, con ragionevole certezza, quali condotte siano penalmente rilevanti. Sotto questo profilo, la nozione di "misure tecniche idonee a prevenire malfunzionamenti" non soddisfa questo requisito. A differenza dei tradizionali reati di pericolo, l'adeguatezza delle misure di sicurezza nel campo dell'IA dipende da standard tecnici in continua evoluzione, dal contesto specifico di utilizzo e da valutazioni probabilistiche su cui persino gli esperti non concordano.

La disposizione non è dunque in grado di soddisfare il canone di determinatezza che il diritto penale esige.

3.2 Violazione dei diritti di difesa e del giusto processo

Anche i diritti di difesa e a un processo equo, garantiti dall'ordinamento italiano e dalla Carta dei Diritti Fondamentali dell'UE, risultano strutturalmente compromessi, sotto due profili distinti.

1. **Nel procedimento penale** che scaturirebbe dal decreto, l'imputato non sarebbe in grado di conoscere *ex ante* lo standard di condotta che è tenuto a rispettare. Infatti le "misure tecniche idonee" non sarebbero note al momento della progettazione e dell'immissione sul mercato del sistema: lo standard verrebbe costruito soltanto in sede processuale, **privando così l'imputato di qualsiasi possibilità di orientare la propria condotta secondo la legge.**
2. **Nel procedimento civile, la combinazione di tre elementi genera un'architettura processuale tale da rendere sostanzialmente impossibile per il convenuto liberarsi dalla responsabilità:** (i) la facoltà del giudice di ordinare la divulgazione della documentazione tecnica relativa al funzionamento del sistema ai sensi del Regolamento (UE) 2024/1689; (ii) la presunzione di ammissione dei fatti allegati dalla controparte in caso di mancata divulgazione, per qualsiasi ragione ritenuta ingiustificata dal giudice; (iii) l'esclusione della conformità al Regolamento (UE) 2024/1689 come esimente nelle azioni civili. Sebbene il decreto preveda formalmente un criterio di proporzionalità e tutele in materia di segreti commerciali, il meccanismo complessivo risulta incompatibile con il principio della parità delle parti sancito dall'art. 6 CEDU, ponendo il convenuto in una **condizione di sostanziale assenza di difesa praticabile.**

Il decreto rischia infine di non rispettare - nella sostanza - il principio di separazione dei poteri: in assenza di standard predefiniti da parte degli organismi tecnici o delle autorità di

regolamentazione competenti, saranno i tribunali italiani a definire cosa significa sicurezza dell'IA in Italia.

3.3 Indeterminatezza della fattispecie di alterazione

Il comma 2 dell'articolo 437-bis punisce altresì chiunque alteri il sistema stesso. Tuttavia, né il decreto in oggetto, né l'AI Act forniscono alcuna definizione di "alterazione". Il termine è potenzialmente idoneo a ricomprendere attività di routine - quali aggiornamenti software, modifiche al modello o attività di testing - che non solo sono comunemente effettuate, ma risultano essenziali per il funzionamento sicuro ed efficace dei sistemi di intelligenza artificiale.

Ciò determina due distinti ordini di problemi. In primo luogo, la disposizione impone a fornitori e deployer un obbligo di prevenire l'alterazione del sistema successivamente alla sua immissione sul mercato: un obbligo che è tecnicamente impossibile adempiere una volta che il sistema si trova nella disponibilità di utenti a valle della catena distributiva. In secondo luogo, essa rischia di esporre un soggetto a responsabilità penale per alterazioni compiute da terzi sui quali non esercita alcun controllo operativo, in violazione del principio di personalità della responsabilità penale.

Occorre inoltre sottolineare che l'AI Act disciplina già questo profilo attraverso il proprio regime delle "**modifiche sostanziali**". Il decreto dovrebbe pertanto allinearsi a tale impostazione, anziché introdurre una fattispecie parallela e priva di definizione che criminalizza condotte che il soggetto non ha posto in essere e non avrebbe potuto impedire.

4. Sproporzione della pena e violazione del principio di proporzionalità

4.1 Disallineamento rispetto al quadro sanzionatorio dell'AI Act e alla prassi degli Stati Membri

Il regime sanzionatorio dell'AI Act è costruito su sanzioni amministrative pecuniarie e misure di vigilanza. Pur riconoscendo agli Stati Membri discrezionalità in materia penale, il Regolamento europeo calibra il proprio apparato sanzionatorio attraverso strumenti amministrativi, muovendo dalla premessa che le violazioni di natura tecnica, anche gravi, siano ontologicamente diverse dalle condotte meritevoli di pena detentiva. L'approccio italiano si discosta significativamente da tale impostazione sotto diversi profili:

- rende penalmente perseguibili le omissioni anziché l'uso intenzionalmente illecito, prevedendo pene detentive per le persone fisiche e sanzioni pecuniarie per gli enti;
- introduce la responsabilità da "pericolo concreto", fondata su una possibilità di danno piuttosto che sull'effettivo verificarsi dello stesso;
- prevede esplicitamente che la conformità al Regolamento (UE) 2024/1689 non esclude di per sé la responsabilità del convenuto in Italia;

- estende la responsabilità penale alla condotta colposa, con la conseguenza che decisioni tecniche adottate in buona fede possono essere oggetto di procedimento penale.

In base al principio costituzionale di proporzionalità, la severità delle sanzioni penali deve avere un rapporto razionale con la gravità della condotta e il grado di colpevolezza. Tale rapporto non è tuttavia ravvisabile nell'impianto del decreto legislativo.

Vale la pena evidenziare che nessun altro Stato Membro dell'UE ha adottato un approccio analogo: la Danimarca, unico altro Paese ad aver introdotto disposizioni penali nell'attuazione dell'AI Act fino ad oggi, si è limitata alle sanzioni pecuniarie.

L'Italia rischia di diventare un caso isolato - non perché attribuisce maggiore serietà alle istanze di sicurezza, ma perché lo strumento scelto è sproporzionato rispetto all'obiettivo perseguito e, pertanto, contrario ai principi fondamentali della responsabilità penale.

4.2 Imputazione causale e violazione del principio di personalità della responsabilità penale

Il decreto presenta inoltre un ulteriore vizio di fondo: **confonde due fonti di pericolo ontologicamente distinte - la progettazione di un sistema e la decisione deliberata di un utente di impiegare per scopi dannosi**. Secondo i principi fondamentali della responsabilità penale, il danno deve essere causalmente collegato al suo effettivo autore, non all'architettura del sistema. Il decreto, tuttavia, anziché procedere all'accertamento - più complesso ma giuridicamente corretto - della persona che ha effettivamente causato il danno e stabilire il suo dolo, costruisce artificialmente un nesso causale con il progettista o il *deployer* del sistema.

L'errata attribuzione della responsabilità viola i principi della personalità della responsabilità penale, di prevedibilità (articoli 25 e 27 della Costituzione) e di necessità del nesso causale (articolo 40 del Codice penale): uno sviluppatore non può ragionevolmente prevedere - e quindi essere penalmente responsabile per - la gamma potenzialmente illimitata di usi malevoli a cui un terzo malintenzionato potrebbe destinare un sistema *general-purpose*.

Il decreto aggrava ulteriormente tale problematica estendendo la responsabilità penale a "chiunque" sia, in senso lato, coinvolto nell'utilizzo di un sistema di intelligenza artificiale ad alto rischio. L'AI Act, al contrario, ripartisce gli obblighi in modo specifico in base al ruolo dell'operatore, attribuendo a ciascun soggetto doveri distinti e delimitati, proporzionati all'effettivo controllo operativo esercitato. La locuzione "chiunque" adottata dal decreto rompe questo impianto e genera un'ambiguità in merito all'esposizione penale dei soggetti operanti lungo la più ampia catena del valore. Essa rischia inoltre di sottoporre più entità appartenenti al medesimo gruppo societario a una responsabilità penale parallela per la stessa omissione, sebbene una sola di esse possa aver esercitato un effettivo controllo operativo sull'obbligo rilevante. **Ricondurre la responsabilità penale ai ruoli definiti dall'AI Act e all'effettivo**

controllo operativo esercitato dal soggetto chiamato a rispondere risulta coerente con i requisiti costituzionali in materia di personalità della responsabilità penale.

4.3 Sproporzione delle sanzioni accessorie

Il decreto assoggetta le aziende all'intero spettro delle sanzioni interdittive previste dal decreto legislativo n. 231 del 2001, ivi incluso il divieto di pubblicizzare beni o servizi. Tale sanzione non presenta alcun nesso razionale con la condotta contestata - la mancata adozione di adeguate misure di sicurezza - e risulterebbe manifestamente sproporzionata, in particolare nei casi in cui non si sia verificato alcun danno effettivo. L'articolo 9, comma 2, del decreto legislativo n. 231 del 2001 richiede che le sanzioni interdittive siano proporzionate alla natura e alla gravità dell'illecito. Si ritiene opportuno sottolineare inoltre che il divieto di pubblicità è stato tradizionalmente limitato alle fattispecie direttamente connesse all'attività di comunicazione commerciale.

La sanzione interdittiva in questione dovrebbe essere quindi applicata previa verifica giudiziale della sussistenza di un nesso di strumentalità diretta tra l'attività pubblicitaria o di comunicazione commerciale dell'ente e la commissione o l'occultamento del reato presupposto.

5. Il quadro in concreto: l'operatore diligente senza safe harbour

Si consideri la posizione di un'azienda che abbia:

- pienamente attuato i requisiti del Regolamento (UE) 2024/1689
- ottenuto la certificazione attraverso la procedura di valutazione della conformità
- implementato robuste misure di sicurezza e di sorveglianza umana

In base al decreto, tale azienda può comunque essere soggetta a procedimento penale - poiché "misure tecniche idonee" e "pericolo concreto" restano concetti indefiniti - e può comunque essere soggetta a responsabilità civile dal momento che la conformità al Regolamento (UE) 2024/1689 non costituisce una difesa nelle cause civili, e qualsiasi non conformità tecnica, per quanto minore, fa scattare una presunzione di causalità in una causa civile.

Proposte

Le criticità esposte richiedono interventi specifici sul testo. Le proposte che seguono mirano a rendere il decreto costituzionalmente solido, proporzionato rispetto agli obiettivi dell'AI Act e coerente con i principi fondamentali della responsabilità penale, senza rinunciare all'obiettivo di garantire elevati standard di sicurezza per i sistemi di IA ad alto rischio.

1. all'**articolo 12**, la fattispecie di cui all'articolo 437-bis del codice penale dovrebbe essere riformulata in modo da: ricondurre la responsabilità penale ai ruoli definiti dall'articolo 3 del regolamento (UE) 2024/1689, nella misura in cui gli obblighi siano applicabili al ruolo ricoperto e nell'ambito dell'effettivo controllo operativo esercitato sul sistema; ancorare la

valutazione del pericolo concreto alla mancata adozione di misure di gestione del rischio appropriate e mirate ai sensi dell'articolo 9 del regolamento (UE) 2024/1689; subordinare la rilevanza penale dell'omissione alla violazione di un obbligo specificamente applicabile al soggetto ai sensi del medesimo regolamento o dei relativi atti di esecuzione; **subordinare la rilevanza penale dell'omissione alla violazione di un obbligo specificamente applicabile al soggetto ai sensi del medesimo Regolamento o dei relativi atti di esecuzione;**

2. all'**articolo 17**, l'ordine di esibizione nei confronti di terzi estranei al giudizio dovrebbe essere subordinato alla sussistenza cumulativa dei seguenti presupposti: che gli elementi di prova richiesti non possano essere ragionevolmente ottenuti dall'altra parte; che il terzo sia stato direttamente coinvolto nella progettazione, nell'addestramento, nell'immissione sul mercato o nell'utilizzo dello specifico sistema di intelligenza artificiale ad alto rischio oggetto della domanda; che l'ordine sia limitato agli elementi di prova direttamente rilevanti rispetto al funzionamento dello specifico sistema nel contesto in cui si è verificato il danno lamentato e sia proporzionato rispetto agli interessi legittimi del terzo, ivi compresa la tutela dei segreti commerciali ai sensi della direttiva (UE) 2016/943 e della documentazione tecnica soggetta agli obblighi di riservatezza previsti dall'articolo 78 del regolamento (UE) 2024/1689;
3. all'**articolo 18**, la presunzione del nesso di causalità dovrebbe essere riformulata in modo da subordinarne l'operatività alla prova, posta a carico dell'istante, dei seguenti elementi: il verificarsi, in capo al convenuto, di un incidente grave ai sensi dell'articolo 3, comma 1, numero 49, del regolamento (UE) 2024/1689; il verificarsi di un danno riconducibile alla tipologia lamentata; la riconducibilità del danno lamentato alla tipologia di danno normalmente derivante dall'obbligo di cui è accertata la violazione; ferma restando la facoltà del convenuto di confutare la presunzione mediante prova contraria, in coerenza con l'impostazione adottata dalla direttiva (UE) 2024/2853 in materia di responsabilità per danno da prodotti difettosi;
4. all'**articolo 19**, dovrebbe essere introdotta una presunzione relativa di assenza di colpa a favore del convenuto che dimostri il rispetto degli obblighi applicabili al proprio ruolo ai sensi del regolamento (UE) 2024/1689, inclusa l'avvenuta positiva conclusione della pertinente procedura di valutazione della conformità di cui al Capo V del medesimo regolamento;

Si auspica inoltre l'adozione di misure volte a:

- **assicurare adeguate competenze tecniche nei procedimenti giudiziari.** Laddove i tribunali siano chiamati a valutare l'adeguatezza tecnica di un sistema di IA, dovrebbe essere garantito il coinvolgimento di consulenti tecnici d'ufficio (CTU) o il rinvio alle determinazioni delle autorità di regolamentazione competenti. Ciò garantirebbe che le decisioni siano fondate su elementi tecnici, piuttosto che su ipotesi giudiziarie non adeguatamente informate.
- **garantire la proporzionalità della pena.** L'applicazione di pene detentive fino alla reclusione da tre a dieci anni rischia di equiparare le omissioni colpose in materia di sicurezza dell'IA a gravi reati dolosi - una sproporzione difficile da conciliare con i principi fondamentali del diritto penale, in particolare il principio di proporzionalità della pena.

Sarebbe pertanto opportuno prevedere un sistema graduato di interventi e sanzioni, che riflettano l'effettivo grado di colpevolezza, partendo da misure amministrative e arrivando alla responsabilità penale solo per le condotte intenzionali più gravi. Un approccio di questo tipo consentirebbe di dotare la magistratura di strumenti calibrati sull'effettivo disvalore della condotta.