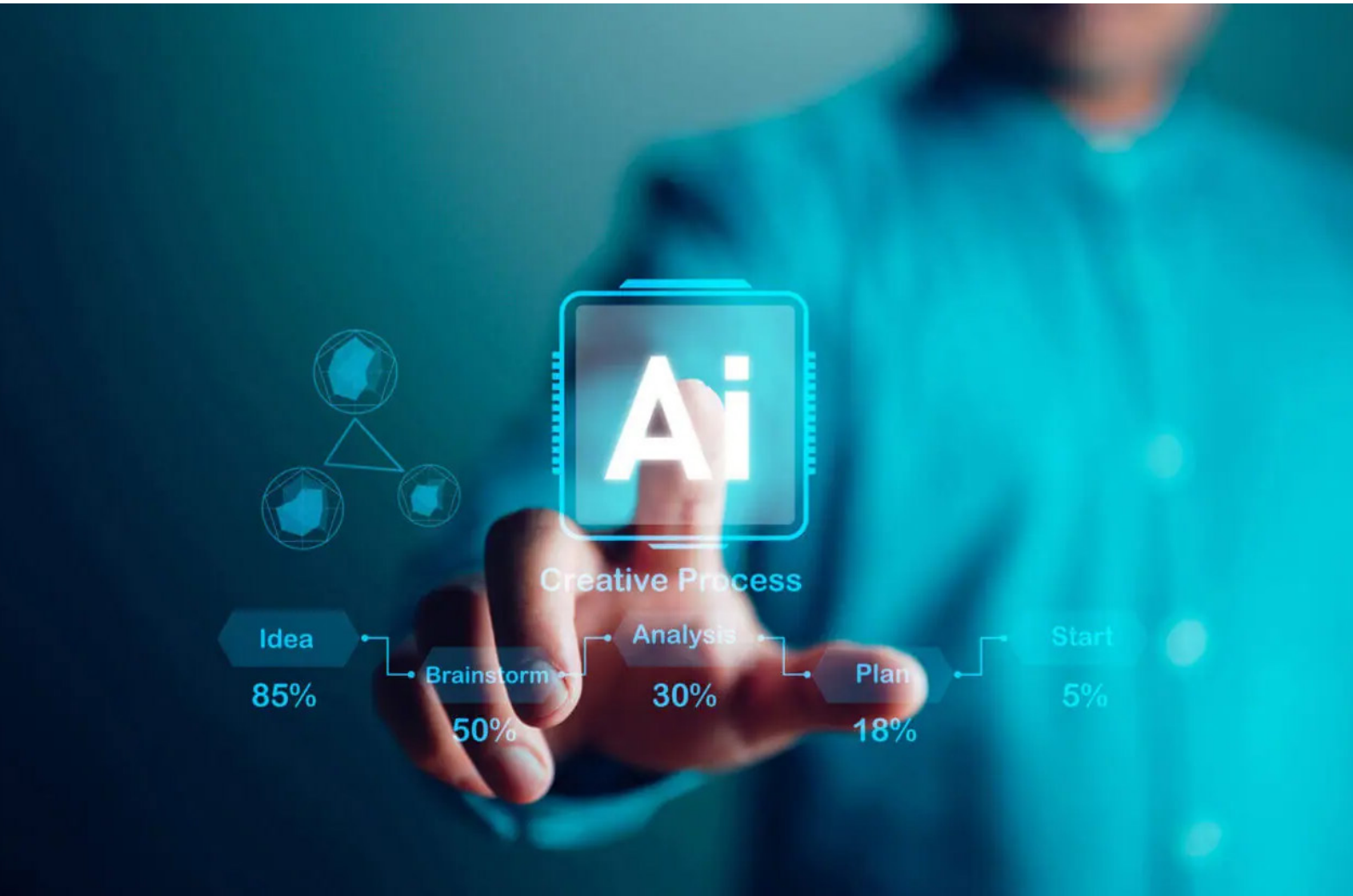
AI Act e responsabilità penale: cosa cambia per provider e deployer

Testi a cura di:

Silvia Stefanelli
Studio Legale Stefanelli & Stefanelli

Anna Terrizzi
Studio Legale Stefanelli & Stefanelli



INDICE DEGLI ARGOMENTI

L'entrata in vigore del'**AI Act**, primo apparato normativo al mondo a disciplinare lo sviluppo, l'immissione sul mercato e l'uso dei sistemi di intelligenza artificiale, è ormai imminente.

Nonostante, ad oggi, in tema di responsabilità il dibattito si focalizzi perlopiù sui **rimedi civilistici** – che, per le loro caratteristiche, rappresentano uno strumento particolarmente efficace per la tutela dei soggetti danneggiati dai sistemi artificiali – l'avvento dell'IA è destinato ad impattare anche sul versante della responsabilità penale.

Nei nostri precedenti contributi abbiamo già effettuato una dettagliata **ricognizione dei soggetti coinvolti dall'AI Act**. In questo articolo evidenzieremo, quindi, gli scenari aperti dal Regolamento con particolare riferimento alle implicazioni penalistiche per le figure del **provider** e del **deployer**.

1

PROVIDER E DEPLOYER NELL'AI ACT: RUOLI E DEFINIZIONI

Provider e deployer: chi sono?

Nell'intento di promuovere la diffusione di un'intelligenza artificiale sicura ed affidabile, il nuovo Regolamento detta specifiche regole non solo in capo ai fornitori dei sistemi di IA (i c.d. **providers**), ma anche ai loro utilizzatori (i c.d. **deployers**).

Partiamo quindi dalle definizioni.

Introdotte dall'art. 2, le figure del fornitore e dell'utilizzatore vengono poi ulteriormente specificate dall'art. 3, che ne traccia il perimetro di operatività.

Secondo la versione finale dell'A.I. Act:

- Il ***provider*** è "una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito";

- Il ***deployer*** è invece la "persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale".

Il regolamento, pertanto, si riferisce **non solo all'utilizzatore persona fisica, ma anche alle entità** – incluse le P.A. – che utilizzano o rendono disponibili sotto la propria autorità sistemi di IA agli utenti sul mercato, esclusi i fornitori o gli importatori, tranne nei casi di utilizzo personale non professionale.

Fondamentali, a questo proposito, due precisazioni:

1. il Regolamento si applica anche a providers e deployers di sistemi di IA stabiliti o situati in un **paese terzo**, in tutti i casi in cui l'output prodotto dal sistema venga utilizzato all'interno del territorio dell'Unione (art. 2, par. 1, lett. c);
2. ai sensi del Considerando 84, in specifiche circostanze (ad esempio: nel caso in cui venga apportata una modifica sostanziale a un sistema di IA ad alto rischio o nel caso in cui se ne modifichi la destinazione d'uso) qualsiasi distributore, importatore, utilizzatore o altra terza parte ("deployer") viene considerato un fornitore ("provider"). In tal caso, dato che **il ruolo di fornitore (provider) verrà concretamente assunto dal deployer, in capo a quest'ultimo ricadranno, di conseguenza, gli obblighi e le responsabilità che il Regolamento attribuisce al provider**. Sono però "fatte salve le disposizioni più specifiche stabilite in alcune normative di armonizzazione dell'Unione basate sul nuovo quadro legislativo, unitamente al quale dovrebbe applicarsi il presente regolamento. Ad esempio, l'articolo 16, paragrafo 2, del regolamento (UE) 2017/745, che stabilisce che talune modifiche non dovrebbero essere considerate modifiche di un dispositivo tali da compromettere la sua conformità alle prescrizioni applicabili, dovrebbe continuare ad applicarsi ai sistemi di IA ad alto rischio che sono dispositivi medici ai sensi di tale regolamento".

2. OBBLIGHI E RESPONSABILITÀ DEI PROVIDER SECONDO L'AI ACT

Quali sono i loro obblighi?

In base alla qualificazione in termini di provider o deloyer, l'AI Act contempla una serie diversi obblighi e responsabilità.

Sotto tale profilo, ruolo fondamentale va attribuito alla **classificazione dei sistemi di IA in base al rischio legato al loro utilizzo**. Infatti, in ossequio ad un approccio marcatamente "*risk-based*" – elemento caratterizzante della nuova disciplina regolatoria – **maggiore è il rischio che l'utilizzo del sistema può comportare per l'utente, più stringente risulterà la relativa regolamentazione.**

Il Regolamento accorda particolare rilevanza ai **sistemi ad alto rischio** (art.6) – nel cui novero rientrano anche i dispositivi medici, in virtù del richiamo alla normativa di armonizzazione contenuto e nell'All. I, cui l'art. 6, par. 1, lett. a, rimanda espressamente) – imponendo ai ***providers*** specifici adempimenti.

Tra gli **obblighi previsti in capo al provider dei sistemi ad alto rischio**, elencati all'art. 16, si annoverano, ad esempio:

- garantire che i loro sistemi siano conformi ai requisiti espressamente previsti dal Regolamento;
- dotarsi di un sistema di gestione della qualità;
- conservare i log generati automaticamente dai sistemi di ad alto rischio, quando sono sotto il loro controllo;

- garantire che il sistema sia sottoposto alla procedura di valutazione della conformità prima della sua immissione sul mercato o messo in servizio;
- elaborare una dichiarazione di conformità UE e apporre la marcatura CE sul sistema di IA ad alto rischio oppure, ove ciò non sia possibile, sul suo imballaggio o sui documenti di accompagnamento per indicare la conformità al regolamento;
- rispettare gli obblighi di registrazione;
- adottare le necessarie misure correttive e fornire le informazioni necessarie;
- dimostrare, su richiesta motivata di un'autorità nazionale competente, la conformità del sistema di IA ad alto rischio ai requisiti del Regolamento;

Il Considerando 73 demanda, inoltre, al provider l'**individuazione di misure di sorveglianza umana** (art. 14) adeguate, prima dell'immissione del sistema sul mercato o della sua messa in servizio. Queste dovranno dunque "garantire, ove opportuno, che il sistema sia soggetto a vincoli operativi intrinseci che il sistema stesso non può annullare e che risponda all'operatore umano, e che le persone fisiche alle quali è stata affidata la sorveglianza umana dispongano delle competenze, della formazione e dell'autorità necessarie per svolgere tale ruolo".

3 I DOVERI DEI DEPLOYER SOTTO L'AI ACT

I providers di sistemi di IA sono responsabili della conformità dei loro sistemi ai criteri stabiliti dall'AI ACT soprattutto in termini di sicurezza, affidabilità e trasparenza, ma il Regolamento introduce **specifiche regole per anche per i deployer, in qualità di utilizzatori dei sistemi di IA.**

Ai sensi dell'art. 26 **tra i principali obblighi cui è tenuto il deployer del sistema di IA ad alto rischio**, rientrano:

- **adottare** idonee misure tecniche e organizzative a garanzia dell'utilizzo dei sistemi, conformemente alle istruzioni per l'uso fornite dai providers;
- **affidare** la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario;
- **monitorare** il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso e, se del caso, informare i fornitori a tale riguardo;
- **informare** senza ritardo il fornitore o il distributore e la pertinente autorità di vigilanza del mercato, sospendendone l'uso, qualora abbiano motivo di ritenere che l'uso del sistema di IA ad alto rischio in conformità delle istruzioni possa presentare un rischio per la salute, la sicurezza o i diritti fondamentali delle persone;
- **informare** immediatamente il fornitore e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato, qualora abbiano individuato un incidente grave.

4

L'IMPATTO IN TERMINI DI RESPONSABILITÀ PENALE

Dalla panoramica appena svolta, si evince come l'AI Act predisponga, per providers e deployers dei sistemi di IA, un articolato ventaglio di standard di comportamento e obblighi di conformità e trasparenza, la cui violazione è sanzionata con la (sola) **irrogazione di sanzioni amministrative pecuniarie** il cui ammontare, nel rispetto dei parametri fissati dal Regolamento (artt. 99/101), sarà stabilito dai singoli Stati membri.

Grande assente dal nuovo assetto normativo è invece la responsabilità penale, con riferimento alla quale – in attesa di interventi legislativi di adeguamento – dovrà farsi riferimento alla disciplina esistente.

Vediamo quale.

Obblighi e attività funzionali alla gestione del rischio

Il sistema predisposto dall' **AI Act promuove un intervento di tipo "proattivo", più che "reattivo"**, imponendo ai soggetti coinvolti (e quindi, nella gran parte dei casi, alle imprese) una serie di **obblighi e di attività funzionali alla gestione del rischio**, che danno vita ad un articolato sistema di responsabilità.

In conformità all'approccio "risk-based", il Regolamento – pur privo di efficacia diretta in materia penale – delimita infatti un'**area di rischio consentito**, individuando una serie di requisiti in presenza dei quali il sistema di IA può

considerarsi conforme e che saranno, dunque, quelli cui le imprese dovranno conformarsi per produrre e immettere sul mercato.

Il ruolo della compliance

In ottica di adeguamento alle nuove disposizioni dell' AI ACT decisivo sarà, quindi, il ruolo della **compliance**.

Sotto questo profilo, sarà fondamentale operare una **preventiva valutazione dei possibili rischi legati alle attività svolte da o tramite i sistemi di IA, che andranno "contenute" nei limiti del rischio consentito**. Predisposte le adeguate cautele preventive, la responsabilità per gli eventi dannosi/pericolosi eventualmente verificatisi in conseguenza del loro mancato rispetto, sarebbe quindi imputabile in capo ai singoli soggetti preposti alla loro adozione, nonché all'ente.

I modelli di organizzazione e gestione (MOG) ex. D.lgs. 231/01

Un ausilio concreto, in funzione di controllo del rischio, potrebbe allora individuarsi nei **modelli di organizzazione e gestione (MOG) ex. D.lgs. 231/01** attraverso i quali identificare le figure apicali cui spetta potere decisionale e le stesse modalità di intervento per le ipotesi in cui il reato – rientrante tra i reati "presupposto" della della responsabilità amministrativa dell'ente – venga in essere in conseguenza dell'utilizzo del sistema di IA.

Come ribadito anche dalla Cassazione, in presenza di un assetto organizzativo oggettivamente negligente nell'adottare le cautele necessarie a prevenire la commissione dei reati, l'evento dannoso è imputabile all'ente per "colpa di organizzazione" e nei suoi confronti potranno quindi essere comminate le sanzioni previste dal D.Lgs. 231/2001.

Come anticipato, il Regolamento nulla stabilisce invece in ottica "reattiva": **sebbene l'impiego di sistemi di IA possa dar vita alla commissione di fatti illeciti, il legislatore europeo non prevede alcun obbligo di incriminazione.**

Tuttavia, ciò non ne esclude la possibile ricorrenza.

Sotto tale punto di vista, nell'individuazione delle fattispecie di reato configurabili, è essenziale evidenziare come il fatto illecito possa avere rilevanza sia nella **dimensione individuale**, che **collettiva**.

5. LE SANZIONI DEL CODICE DEL CONSUMO

Infatti, in quanto generalmente prodotti in serie, i prodotti sono immessi sul mercato in grandi quantità e l'eventuale difettosità, non conformità o alterazione del loro stato fa sorgere un pericolo per la salute, l'incolumità o addirittura per la vita nei confronti non di un individuo, ma di una **collettività indistinta**. Fondamentale importanza rivestono, quindi, le sanzioni previste dalla legislazione speciale di protezione dei consumatori, ossia dal **Codice del consumo** (D.lgs. 206/2005).

Tra queste, in ambito penalistico, particolarmente rilevante è l'**art. 112, comma 2, del Cod. cons.**, ai sensi del quale "salvo che il fatto costituisca più grave reato, il produttore che immette sul mercato prodotti pericolosi è punito con l'arresto fino ad un anno e con l'ammenda da 10.000 euro a 50.000 euro". Il provider, dunque, potrebbe essere chiamato a rispondere ai sensi della predetta disposizione, tutte le volte in cui immettesse sul mercato un prodotto non rispondente alla definizione di "prodotto sicuro".

Alla dimensione collettiva si unisce, poi, quella **individuale**, relativa al pericolo o al danno che il prodotto può arrecare al singolo utente.

Con riferimento a tale ipotesi, benché non siano previste norme ad hoc a protezione del consumatore, possono comunque configurarsi le fattispecie di reato contro la vita e l'incolumità individuale.

Tra queste, le fattispecie di **omicidio e lesioni personali** – anche (e soprattutto) in **forma colposa** – sono quelle suscettibili di trovare maggiore applicazione, perché idonee a **tutelare gli interessi personali del soggetto che subisca un danno o incorra in un pericolo per la propria vita/per la propria incolumità, in conseguenza dell'uso del prodotto che presenti difetti o alterazioni.**

6. SORVEGLIANZA UMANA E RESPONSABILITÀ NEL CONTESTO DELL'AI ACT

Particolarmente rilevante, sotto questo aspetto, il concetto di **human oversight**, (art. 14). La **sorveglianza umana** – che ha l'obiettivo di " prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile" – viene infatti **realizzata non solo mediante misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore (provider) prima della sua immissione sul mercato o messa in servizio, ma anche attraverso misure che, individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio, siano adatte ad essere attuate dal deployer.**

In virtù del ruolo centrale riconosciuto alla sorveglianza, dal punto di vista penalistico, potrebbe dunque prospettarsi una **responsabilità del "sorvegliante umano"** – sia esso provider o deployer – **per l'omessa adozione di idonee misure volte ad impedire gli eventi lesivi verificatisi per effetto dell' "agire" del sistema di IA.**

NETWORK DIGITAL 360

Network Digital360 è il più grande network in Italia di testate e portali B2b dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale, con oltre 50 fra portali, canali e newsletter.
Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane e di fornire a tutti i decisori che devono valutare investimenti tecnologici informazioni aggiornate e approfondite.
Il Network è parte integrante di Digital360HUB, il polo di Demand Generation di Digital360, che mette a disposizione delle tech company un'ampia gamma di servizi di comunicazione, storytelling, pr, content marketing, marketing automation, inbound marketing, lead generation, eventi e webinar.

VIA COPERNICO, 38
20125 - MILANO
TEL. 02 92852785
MAIL: MARKETING@DIGITAL4.BIZ