DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

La responsabilità del deployer nell'uso dell'Intelligenza Artificiale

17 Dicembre 2024

Mariafrancesca De Leo, Partner, Greenberg Traurig Santa Maria
Bertone Biscaretti di Ruffia, Senior Associate, Greenberg Traurig Santa Maria

DB non solo diritto bancario

Mariafrancesca De Leo, Partner, Greenberg Traurig Santa Maria

Bertone Biscaretti di Ruffia, Senior Associate, Greenberg Traurig Santa Maria

Mariafrancesca De Leo

Mariafrancesca De Leo è partner dell'ufficio di Milano di Greenberg Traurig. Si occupa prevalentemente di contenzioso in ambito finanziario, di profili regolamentari, nonché di indagini interne, relative ad abusi di mercato, violazione di sistemi e controlli e di episodi corruttivi. Si inoltre di contenziosi societari e commerciali nel settore industriale, in quello energetico e tecnologico.

Il Regolamento dell'Unione Europea sull'Intelligenza Artificiale (il Regolamento) è entrato in vigore il 1° agosto 2024, introducendo requisiti stringenti e nuovi profili di responsabilità per i diversi attori nella catena di valore dell'Intelligenza Artificiale (IA).

Il Regolamento adotta innanzitutto un approccio basato sul rischio, fondato sul principio per cui maggiore sono i rischi insiti nell'utilizzo di un particolare sistema di IA, più stringente sarà il regime regolatorio applicabile. In quest'ottica, sono ad esempio proibiti quei sistemi che comportano rischi considerati inaccettabili, mentre i sistemi di IA considerati ad alto rischio soggiacciono a requisiti particolarmente rigorosi e una normativa speciale è dedicata alle IA per finalità generali.

Ma gli obblighi e i requisiti applicabili agli operatori del settore sono gradati anche in base al ruolo che questi ricoprono rispetto alla realizzazione, alla commercializzazione e all'uso di un determinato sistema di IA, o di un prodotto o servizio che lo incorpora.

L'ambito di applicazione del Regolamento è infatti particolarmente ampio. Esso si applica a tutti gli operatori del settore nel mercato dell'Unione Europea, dai fornitori agli importatori e i distributori, dai fabbricanti di prodotti che incorporano sistemi di IA forniti da terzi, fino agli utilizzatori finali, i c.d. *deployer*.

Quest'ultima figura, in particolare, ampia notevolmente il perimetro applicativo del Regolamento, in quanto ricomprende tutte le persone fisiche o giuridiche che utilizzino un sistema di IA sotto la propria autorità, anche qualora siano stabiliti in un paese extra UE, nella misura in cui l'output prodotto da tale sistema sia destinato a essere utilizzato nell'Unione. Restano infatti esclusi da tale definizione esclusivamente quei soggetti che facciano dell'IA un uso personale non professionale[1].

Sia il riferimento all'autorità sotto la quale viene svolto l'utilizzo dell'IA, sia l'espressa esclusione del solo uso personale e strettamente non professionale, generano assonanze con la definizione di titolare del trattamento e, più in generale, con il GDPR, il Regolamento generale dell'Unione Europea sulla protezione dei dati personali.

1 Cfr. Art. 3(1)(4) del Regolamento.

Entrambe le normative in questione si fondano su un principio di responsabilizzazione (*accountability*) finalizzato, tra l'altro, a fare sì che i soggetti eventualmente danneggiati possano sempre individuare il soggetto responsabile, demandando a quest'ultimo l'obbligo di dimostrare la propria *compliance* con le norme di settore.

Tutto ciò porta a concludere che gli obblighi previsti per i deployer siano applicabili non solo a quei soggetti che offrono ai propri clienti o al pubblico servizi e prodotti basati sull'IA, ma anche a tutte quelle imprese il cui business principale non ha niente a che fare con tale tecnologia e che utilizzano sistemi di IA forniti da terzi per attività accessorie come, ad esempio, il reclutamento, l'assistenza ai clienti o la gestione organizzativa.

Alla definizione di deployer, d'altronde, si contrappone quella di fornitore (provider), definito come ogni soggetto che sviluppa, o fa sviluppare, un sistema di IA e lo immette sul mercato, o lo mette in servizio con il proprio nome o marchio, a titolo oneroso o gratuito[2].

L'importanza di qualificare correttamente il proprio ruolo quale deployer piuttosto che quale provider

Il provider e il deployer costituiscono solo due delle diverse figure individuate dal Regolamento e alle quali corrispondono obblighi e requisiti diversi.

Distinguere tra i due ruoli, tuttavia, è particolarmente rilevante sia perché si tratta delle figure destinatarie dei principali obblighi imposti dal legislatore europeo, ad esempio, per quanto riguarda la formazione obbligatoria in materia di IA e l'utilizzo dei sistemi considerati ad alto rischio, sia perché il ruolo del deployer può facilmente sconfinare in quello del fornitore, con conseguenze determinanti in termini di obblighi applicabili.

Alcuni obblighi, infatti, sono comuni a entrambe le figure in questione. È il caso dell'**obbligo di alfabetizzazione**, che impone a entrambi di adottare misure idonee per garantire che il proprio personale sia dotato di un sufficiente livello di conoscenza in materia di IA, in modo tale da essere posto nelle condizioni di prendere decisioni informate in merito ai sistemi di IA con i quali, o sui quali, è chiamato a lavorare[3].

Indipendentemente dal livello di rischio, inoltre, provider e deployer sono tenuti a rispettare alcuni obblighi di trasparenza, finalizzati a informare le persone fisiche in merito al funzionamento di determinati sistemi di IA ai quali sono esposte[4].

La maggior parte degli obblighi imposti ai provider, infine, non si applicano ai deployer, i quali sono invece soggetti a obblighi ulteriori e diversi con riferimento, in particolare, all'utilizzo di sistemi di IA ad alto rischio e dei modelli di IA per finalità generali, ossia le c.d. *General Purpose AI* (GPAI), in grado di svolgere con competenza un'ampia gamma di compiti distinti.

Il regime più gravoso previsto per i provider

Quanto ai sistemi di IA ad alto rischio, i provider devono innanzitutto garantire che i sistemi sviluppati o messi sul mercato siano accompagnati da **un adeguato sistema di gestione dei rischi**, il quale deve tradursi in un processo continuo portato avanti per l'intero ciclo di vita del sistema e teso all'identificazione, analisi e stima dei rischi noti e di quelli possibili insiti sia nell'uso corretto, sia in quello improprio ragionevolmente prevedibile, e finalizzato all'adozione delle misure di gestione opportune per fare fronte ai rischi così individuati[5].

Un'ulteriore obbligazione dei provider, non applicabile ai deployer, riguarda la redazione, l'aggiornamento e la conservazione della **documentazione tecnica** atta a dimostrare la conformità del sistema

2 Cfr. Art. 3(1)(3) del Regolamento.

3 Cfr. art. 4 del Regolamento.

4 Cfr. art. 50 del Regolamento. Gli obblighi in questione, tuttavia, sono delineati in maniera diversa a seconda del ruolo del soggetto obbligato. Mentre ai fornitori è imposto di progettare e realizzare i propri sistemi in modo tale da informare gli utenti del fatto di stare interagendo con un'IA, garantendo altresì che i relativi output audio, immagine o video siano marcati *by design* come generati artificialmente, i deployer hanno obblighi informativi analoghi a quelli previsti in materia di privacy. Questi includono l'obbligo di informare gli utenti in merito al funzionamento dei sistemi di IA in grado di riconoscere le emozioni, o dei sistemi di categorizzazione biometrica, così come l'obbligo di rendere noto, nel caso di sistemi in grado di manipolare immagini, audio o video in modo da generare dei c.d. *deep fake*, che il contenuto digitale in questione è stato generato o manipolato artificialmente

5 Cfr. art. 9 del Regolamento.

di IA in questione[6].

I fornitori devono poi garantire, anche nei confronti dei deployer, il rispetto dei **criteri normativi relativi alla qualità dei set di dati** utilizzati per l'addestramento, la convalida e la prova dei sistemi di IA che realizzano e commercializzano, e devono dotare i deployer di **istruzioni per l'uso** che comprendano informazioni concise, complete, corrette e chiare in merito al loro utilizzo. Inoltre, devono garantire, anche nei confronti dei deployer, che i sistemi ad alto rischio siano progettati e realizzati in modo tale da:

i) dotarli di **sistemi di registrazione automatica degli eventi** (*log*);

ii) garantire **un funzionamento sufficientemente trasparente** da consentire ai deployer di interpretarne l'output;

iii) poter essere efficacemente **supervisionati da persone fisiche**;

iv) conseguire un adeguato livello di **accuratezza, robustezza e cybersicurezza**[7].

Ulteriori obblighi dei provider riguardano, oltre alla fase di sviluppo, anche quella di vita del sistema IA. Si tratta, ad esempio, dell'obbligo di istituire un **sistema di gestione della qualità**, mediante l'adozione di *policies* e istruzioni scritte, nonché l'**obbligo di conservazione dei *log*** e quello relativo all'**adozione di una procedura di valutazione della conformità**[8].

La breve disamina così svolta non esaurisce l'elencazione degli obblighi posti in capo a chi sviluppi o immetta sul mercato un sistema di IA, ma rende evidente la complessità del sistema di *compliance* e dei requisiti che i *provider* sono tenuti a rispettare e garantire, anche nei confronti dei deployer.

Gli obblighi dei deployer

Gli obblighi che il Regolamento impone ai deployer riguardano chiaramente l'utilizzo dei sistemi di IA,

6 Cfr. art. 11 del Regolamento.
7 Cfr. artt. 10, 12, 13, 14 e 15 del Regolamento.
8 Cfr. artt. 17, 18, 19 e 43 del Regolamento.

piuttosto che la loro progettazione e messa in commercio, e possono considerarsi meno pervasivi rispetto al complesso regime di *compliance* cui sono soggetti i provider.

Ciò non toglie che anche i deployer dovranno prestare attenzione a una serie di obblighi rilevanti, il cui mancato adempimento può avere conseguenze importanti sia in termini di sanzioni amministrative applicabili, sia in termini di possibili profili di responsabilità civile.

Con riferimento ai sistemi di IA ad alto rischio, essi dovranno ad esempio adottare misure tecniche e organizzative per garantire l'utilizzo dei sistemi di IA in **conformità alle istruzioni d'uso** fornite dai provider e **monitorare il funzionamento** dei medesimi sistemi sulla base di tali istruzioni, nonché affidare la **sorveglianza umana** dei medesimi a persone competenti e formate. Dovranno inoltre garantire che i **dati di input** da essi forniti al sistema di IA siano **pertinenti e sufficientemente rappresentativi** alla luce della finalità del sistema stesso e conservare i log del sistema per un periodo adeguato[9].

Alcune norme sono espressamente dedicate ai deployer attivi in determinati settori. Gli **istituti finanziari** soggetti a requisiti di *governance*, di dispositivi o di processi interni ai sensi della disciplina di settore potranno infatti rispettare gli obblighi di monitoraggio sui sistemi di IA e di conservazione dei relativi *log* adempiendo alle regole di *compliance* imposte dalla normativa in materia di servizi finanziari[10].

In alcuni casi, infine, i deployer sono chiamati a compiere in via preventiva una **valutazione di impatto** sui diritti fondamentali per i sistemi di IA ad alto rischio. È il caso tanto dei deployer che sono soggetti pubblici o che forniscono servizi pubblici, quanto di quei deployer che utilizzano l'IA per svolgere determinate attività tipiche degli istituti assicurativi e finanziari, quali il *risk* e il *credit scoring*[11].

La possibile sovrapposizione tra la figura del deployer e quello del provider

Quanto sopra rende evidente come il Regolamento attribuisca gli obblighi principali ai fornitori dei sistemi di IA.

9 Cfr. art. 26 del Regolamento.
10 Cfr. art. 26(5) e (6) del Regolamento.
11 Cfr. art. 27 del Regolamento.

vedi l'articolo online

La distinzione tra provider e deployer, infatti, non è affatto netta. Il Regolamento prevede espressamente alcune ipotesi in cui un deployer possa essere qualificato anche come provider ed essere dunque tenuto a rispettare, oltre alle obbligazioni gravanti su ogni utilizzatore, anche gli obblighi previsti per i fornitori.

Ciò può accadere, ad esempio, qualora un deployer apponga il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato da un fornitore terzo. È l'ipotesi in cui un provider realizzi un sistema di IA e lo commercializzi quale prodotto o servizio c.d. *white label*, permettendo il *rebranding* da parte dell'acquirente. Il suo cliente, apponendo il proprio brand e utilizzando il medesimo sistema di IA quale deployer, può assumere la qualifica di provider ed essere soggetto al relativo regime regolatorio.

In tale ipotesi, il Regolamento prevede peraltro che il deployer possa evitare il rischio di essere soggetto agli obblighi dei provider adottando idonee misure contrattuali[12].

Il medesimo rischio di essere qualificato come un provider si verifica altresì qualora un deployer modifichi in maniera sostanziale un sistema di IA ad alto rischio, oppure modifichi la finalità prevista di un sistema di IA, comprese le IA per finalità generali, che non sia stato previamente qualificato come sistema ad alto rischio ma lo diventi sulla base della nuova finalità d'uso impressa dal provider[13].

In questi casi divengono evidentemente centrali la nozione di modifica sostanziale e quella di nuova finalità.

Per la prima è necessario fare riferimento in termini generali alla normativa di armonizzazione dell'Unione Europea in materia di conformità e sicurezza dei prodotti e delle macchine, che conosce già da tempo tale nozione, sulla quale si sono sviluppate linee guida e sono state fornite indicazioni interpretative dalla giurisprudenza.

Quanto alla seconda, appare particolarmente rilevante l'individuazione delle finalità nella documentazione tecnica e nelle analisi del rischio predisposte dal provider originario.

12 Cfr. art. 25(1)(a) del Regolamento.
13 Cfr. art. 25(1)(b) e (c) del Regolamento.

La responsabilità lungo la catena del valore dell'IA

La corretta qualificazione di un soggetto come semplice deployer, piuttosto che come provider, non ha conseguenze solo in termini di regime di *compliance* applicabile ai sensi del Regolamento, ma impatta in maniera rilevante anche sui possibili profili di responsabilità civile nei confronti sia degli utenti, sia degli altri operatori nella catena di valore dei sistemi di IA.

Il Regolamento sull'Intelligenza Artificiale, infatti, deve essere letto e interpretato alla luce della normativa vigente in materia di responsabilità civile contrattuale ed extracontrattuale, nonché degli ulteriori testi normativi in materia ai quali il legislatore dell'Unione Europea sta lavorando.

Quanto ai profili di responsabilità contrattuale, un provider sarà normalmente tenuto a garantire sia ai deployer, sia ai propri clienti che non rientrano in tale definizione, il rispetto degli obblighi e dei requisiti imposti dal Regolamento, e dunque a risarcire i danni causati ai sensi dell'art. 1218 c.c. in caso di inadempimento alle obbligazioni descritte nei paragrafi precedenti.

Il mancato rispetto delle medesime obbligazioni ha altresì importanti conseguenze sui possibili profili di responsabilità extracontrattuale.

Sul punto è opportuno fare riferimento alla nuova **direttiva dell'Unione Europea sulla responsabilità per danno da prodotti difettosi**[14], tesa a garantire che, in caso di danni fisici, patrimoniali o perdita di dati causati da sistemi di IA difettosi, sia possibile richiedere il risarcimento al fornitore del sistema di IA o all'operatore che integra tale sistema in un proprio prodotto. Un soggetto qualificato come provider ai sensi del Regolamento sull'Intelligenza Artificiale, infatti, potrebbe essere considerato fabbricante nell'ambito della normativa sui prodotti difettosi e, di conseguenza, essere tenuto a fornire le garanzie previste dalla medesima.

A questo proposito, è da considerare anche la proposta di direttiva del Parlamento europeo relativa

14 Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio (PE/7/2024/REV/1), pubblicata in Gazzetta Ufficiale il 18 novembre 2024.

vedi l'articolo online

all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale[15], con la quale sarà verosimilmente introdotta una presunzione relativa che stabilirà un nesso causale presuntivo tra la violazione di uno specifico obbligo relativo alla fornitura e all'utilizzo di un sistema di IA e l'output fornito dal medesimo.

In altre parole, nel caso in cui un danno sia causato dall'utilizzo di un sistema di IA, al soggetto danneggiato che intenda ottenere un risarcimento potrebbe essere sufficiente dimostrare, oltre al danno, che il provider e/o il deployer coinvolto abbia violato uno dei propri obblighi ai sensi del Regolamento. L'onere di dimostrare che tra tale violazione e il danno subito non ci sia alcun nesso di causalità graverebbe in capo al convenuto, il quale – a seconda delle circostanze del caso – potrebbe liberarsi anche dimostrando di non essere lui il soggetto obbligato a fornire una determinata garanzia, o quantomeno avere la possibilità di farsi manlevare dal proprio fornitore.

In quest'ottica, qualificare correttamente il proprio ruolo nei confronti dei sistemi di IA utilizzati diviene fondamentale per ogni operatore del settore. Da tale qualificazione, infatti, discendono conseguenze sia in termini di obblighi di *compliance* applicabili, sia in termini di possibili responsabilità risarcitorie nei confronti degli altri operatori coinvolti nella filiera e degli utenti finali. Svolgere l'analisi legale necessaria, tuttavia, non sempre sarà facile e richiederà competenze sia legali, sia tecniche, essendo richiesto un buon livello di comprensione, oltre che della nuova normativa in materia, delle caratteristiche e delle modalità di funzionamento dei sistemi di IA coinvolti.

15 Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (COM/2022/496 final).

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it