DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

AI Act: il Regolamento sull'Intelligenza Artificiale adottato dal Parlamento UE

14 Marzo 2024

Italo de Feo, Partner, CMS
Andrea Afferni, Associate, CMS

DB non solo diritto bancario

Italo de Feo, Partner, CMS

Andrea Afferni, Associate, CMS

Italo de Feo

Italo de Feo è Co-Head del dipartimento di TMC – Tecnologie, Media e Comunicazione dello Studio e responsabile del Gruppo Technology internazionale di CMS. Nel corso della sua attività, Italo de Feo ha maturato notevole esperienza in materia di diritto commerciale, diritto delle tecnologie e della proprietà intellettuale, con particolare esperienza in materia di outsourcing di servizi tecnologici, software e licenze, regolamentazione di internet e delle telecomunicazioni, privacy.

Studio Legale

CMS

CMS Law . Tax

Nella giornata di ieri, 13 marzo, il Parlamento europeo ha approvato, con ampia maggioranza, il Regolamento sull'Intelligenza Artificiale (il cosiddetto "**AI Act**"). Il nuovo Regolamento mira a garantire che i sistemi di intelligenza artificiale immessi sul mercato europeo siano sicuri e rispettino i diritti e i valori fondamentali dell'Unione Europea. L'AI Act, inoltre, si pone l'obiettivo di stimolare gli investimenti e l'innovazione nel settore dell'intelligenza artificiale e facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili, posizionando l'UE come uno dei principali attori a livello mondiale. Norme nazionali diverse in ciascun Stato membro dell'UE potrebbero portare alla frammentazione del mercato interno, minacciando il vantaggio competitivo dell'UE, e diminuire la certezza del diritto per gli operatori che sviluppano, importano o utilizzano sistemi di IA all'interno dell'UE.

Il testo del Regolamento approvato dal Parlamento UE conferma l'approccio basato sul rischio già adottato nelle precedenti versioni circolate nei mesi scorsi. Pertanto, vengono imposti obblighi diversificati in base al livello di rischio che ciascuna delle categorie in cui possono essere classificati i sistemi di IA può avere verso i diritti e le libertà degli individui. L'approccio seguito dal Regolamento è, quindi, quello secondo cui maggiore è il rischio, più rigorose sono le regole da applicare.

1. Definizione di "sistema di intelligenza artificiale"

La definizione di "sistema di intelligenza artificiale" contenuta nel Regolamento mira ad essere il più possibile neutrale dal punto di vista tecnologico e adeguata alle esigenze future, tenendo conto dei rapidi sviluppi tecnologici e di mercato relativi all'IA.

Con l'obiettivo di garantire che la definizione fornisca criteri sufficientemente chiari per distinguere l'IA dai sistemi software più semplici e al contempo sia quanto più possibile omogenea rispetto a quelle che, presumibilmente, verranno adottate dai legislatori negli altri paesi nel mondo, l'AI Act allinea la propria definizione con quella adottata precedentemente dall'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE). Il sistema di IA è definito come "*un sistema basato macchine progettato per funzionare con diversi livelli di autonomia, che può mostrare capacità di adattamento dopo l'implementazione e che, per obiettivi espliciti o impliciti, deduce dagli input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici*".

Pertanto, affinché un sistema di IA rientri nella definizione del Regolamento, esso deve:

vedi l'articolo online

(i) essere basato su **macchine** (ovvero sistemi computazionali capaci di generare output) e **progettato con diversi livelli di autonomia**, cioè in grado di operare, almeno in una certa misura, senza l'intervento umano;

(ii) mostrare **capacità di adattamento** e quindi essere dotato dell'abilità di apprendimento che gli permetta di evolvere durante l'uso;

(iv) operare al fine di raggiungere determinati **obiettivi espliciti o impliciti**, quali, ad esempio, la risoluzione di determinati problemi tecnici, la valutazione del merito creditizio di una persona o lo spostamento di un veicolo da un luogo all'altro;

(v) **dedurre come generare output dagli input che riceve** e quindi essere capace di ottenere gli output (ad esempio, previsioni, contenuti, raccomandazioni o decisioni) e di ricavare modelli e/o algoritmi dagli input/dati ricevuti; e

(vi) **influenzare gli ambienti fisici**: gli ambienti sono i contesti in cui opera il sistema di intelligenza artificiale. Ad esempio, un sistema di valutazione del credito influenza il suo ambiente aiutando a decidere se a qualcuno verrà concesso un prestito.

2. Ambito di applicazione

Nel definire ulteriormente l'ambito di applicazione, il Regolamento non sarà applicabile ad aree al di fuori del campo di applicazione del diritto dell'UE. Inoltre, non si applicherà ai sistemi di IA che hanno scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività, nonché ai sistemi di IA utilizzati esclusivamente per scopi di ricerca e innovazione, né alle persone che utilizzano l'IA per scopi non professionali.

Le nuove regole, invece, si applicheranno ai fornitori di sistemi di intelligenza artificiale che immettono sul mercato UE tali sistemi, nonché agli operatori, anche se situati fuori dall'UE, qualora l'output prodotto dal sistema di IA venga utilizzato nel territorio dell'Unione. Sono, infine, ricompresi nell'ambito di applicazione dell'AI Act, anche gli importatori, i distributori, i fabbricanti e i rappresentanti autorizzati di sistemi di IA.

3. Classificazione dei sistemi di IA

Come già accennato, la classificazione dei Sistemi di IA si basa sui rischi identificati per i diritti e le libertà degli individui. In particolare, i sistemi di IA vengono classificati nelle seguenti categorie definite in base ai rischi potenziali: (a) rischio inaccettabile; (b) alto rischio; (c) rischio basso o minimo.

3.1 Rischio inaccettabile

Alcuni usi di sistemi di IA rappresentano una seria minaccia per i diritti fondamentali. Pertanto, il rischio correlato a tali sistemi è considerato inaccettabile dal Regolamento e il loro utilizzo sarà vietato all'interno dell'UE. L'AI Act menziona tra tali sistemi, ad esempio, quelli che possono essere utilizzati per scopi di manipolazione cognitivo-comportamentale dell'utente (ad es. giocattoli che utilizzano assistenti vocali per incoraggiare comportamenti pericolosi nei minori); i sistemi c.d. di "social scoring" o "punteggio sociale", cioè quelli che assegnano un punteggio a ciascun individuo in base al suo comportamento, influenzando in questo modo l'accesso ai servizi, all'occupazione, o ad altre opportunità; quelli che riconoscono le emozioni, se utilizzati sul posto di lavoro e nell'ambito dell'istruzione, i sistemi di identificazione biometrica in tempo reale in spazi accessibili al pubblico; i sistemi di categorizzazione biometrica delle persone fisiche utilizzati per estrarre e elaborare dati sensibili (come l'orientamento sessuale o le credenze religiose) e i sistemi finalizzati alla c.d. "polizia predittiva" e utilizzati per l'elaborazione di previsioni di crimini futuri.

3.2 Alto rischio

In secondo luogo, l'AI Act introduce una serie di previsioni che mirano a garantire che i sistemi di intelligenza artificiale ad alto rischio siano soggetti a rigorosi requisiti e obblighi prima di essere introdotti o utilizzati nell'UE. Questi sistemi includono una vasta gamma di dispositivi, quali quelli utilizzati in infrastrutture critiche, dispositivi medici, nonché sistemi di identificazione biometrica, categorizzazione e riconoscimento delle emozioni. Alla luce del potenziale rischio associato a tali applicazioni, gli obblighi imposti includono l'adozione di sistemi di gestione dei rischi, il rispetto di requisiti relativi alla qualità dei set di dati utilizzati (che deve essere elevata), nonché all'adozione della documentazione tecnica e alla conservazione delle registrazioni, alla trasparenza e alla fornitura di informazioni agli utenti, oltre a prescrivere l'adozione di adeguati livelli di accuratezza, robustezza e cybersicurezza.

vedi l'articolo online

L'AI Act richiede, inoltre, che gli operatori di sistemi di AI ad alto rischio effettuino una valutazione dell'impatto sui diritti fondamentali e che tale valutazione sia effettuata prima che tali sistemi siano immessi sul mercato.

I destinatari di obblighi relativi a sistemi ad alto rischio non sono solo i fornitori di sistemi di IA, ma anche gli altri attori lungo la catena del valore dell'IA (ad esempio importatori, distributori, rappresentanti autorizzati), cui sono imposti obblighi proporzionati.**3.3 Basso rischio**

Il Regolamento sull'IA prevede poi obblighi per i sistemi di IA a basso rischio. Questa categoria include la maggior parte dei sistemi di IA. Il Regolamento chiarisce che la produzione e l'utilizzo di sistemi di intelligenza artificiale che presentano solo un rischio limitato per i diritti e le libertà degli individui saranno soggetti a semplici obblighi di trasparenza. In particolare, l'articolo 52 dell'AI Act stabilisce, in relazione ai sistemi che interagiscono con individui, ai sistemi di riconoscimento delle emozioni e di categorizzazione biometrica non inclusi tra quelli vietati, nonché ai sistemi che generano o manipolano contenuti c.d. "deep fake",, l'obbligo di informare l'utente che sta interagendo con un sistema di intelligenza artificiale o del fatto che un particolare contenuto è stato creato attraverso l'intelligenza artificiale (ad esempio, i contenuti "deep fake" devono essere chiaramente identificati come tali), al fine di consentire all'utente di utilizzare la tecnologia in modo informato e consapevole.

4. Alcune Eccezioni con riferimento alle operazioni delle forze di polizia

Il Regolamento prende attentamente in considerazione le necessità e le specificità relative alle operazioni delle forze di polizia e l'importanza di preservare la loro capacità di impiegare l'IA nel compimento dei loro doveri di tutela della sicurezza pubblica. L'AI Act prevede diverse eccezioni per rispondere a tale necessità. Una delle eccezioni più significative riguarda l'istituzione di una procedura di emergenza, che consentirà alle forze di polizia di utilizzare, solo in situazioni di urgenza, strumenti ad alto rischio di IA, anche ove tali strumenti non avessero superato la valutazione di conformità. Tuttavia, questo meccanismo è accompagnato da misure specifiche per prevenire abusi e garantire il rispetto dei diritti fondamentali. Inoltre, l'utilizzo dei sistemi di IA per l'identificazione biometrica remota in tempo reale negli spazi pubblici è soggetto a una specifica disciplina ed è ammesso solo in casi specifici, come la ricerca di vittime di reati gravi o la prevenzione di atti terroristici o altre minacce alla sicurezza pubblica.

5. Modelli GPAI e foundation models

Importanti previsioni del Regolamento sull'IA sono poi rivolte ai c.d. sistemi di intelligenza artificiale per finalità generali ("**General Purpose AI Model**" o "GPAI"). Si tratta, in particolare, di modelli informatici che, anche tramite l'allenamento su una vasta quantità di dati, possono essere usati per una varietà di compiti, singolarmente o inseriti come componenti in un sistema AI, anche ad alto rischio.

Il nuovo AI Act, in sintesi, prevede una regolamentazione più pervasiva per quei modelli GPAI che possono provocare maggiori rischi sistemici a livello europeo. Negli altri casi, invece, il Regolamento prevede per lo più obblighi di trasparenza, ivi inclusa la messa a disposizione di documentazione tecnica relativa al loro funzionamento e ai processi di data training utilizzati.

6. Codici di condotta volontari per fornitori e utilizzatori di altri sistemi di IA

Il Regolamento ha anche gettato le basi per la creazione di codici di condotta volontari. Ai sensi di questi codici, i fornitori e gli utilizzatori di sistemi di IA a basso rischio potrebbero conformarsi volontariamente a requisiti obbligatori per i sistemi di IA ad alto rischio. Potrebbero anche stabilire e attuare codici che includono impegni volontari, come quelli relativi alla sostenibilità ambientale, all'accessibilità per le persone con disabilità, alla partecipazione degli stakeholder nella progettazione e nello sviluppo dei sistemi di IA, e alla promozione di obiettivi sociali, come la diversità e l'inclusione, la non discriminazione e la prevenzione dell'uso abusivo dei sistemi di IA.

La Commissione europea valuterà l'impatto e l'efficacia dei codici di condotta entro due anni dall'entrata in vigore della legge sull'IA e successivamente ogni tre anni.

7. Governance nell'AI Act

La Commissione europea deve svolgere un ruolo guida nello sviluppo e nell'applicazione delle disposizioni dell'AI Act e vigilare sul loro rispetto. Per questo scopo, il testo del nuovo Regolamento istituisce un quadro di governance nell'ambito del titolo VI, con l'obiettivo di coordinare e sostenere la sua applicazione a livello nazionale. Le misure relative alla governance si applicheranno a partire dai 12 mesi successivi all'entrata in vigore dell'AI Act.

vedi l'articolo online

In particolare, viene istituito un Ufficio per l'IA all'interno della Commissione, con un forte legame con la comunità scientifica a supporto della sua attività. L'Ufficio per l'IA dovrà supervisionare i modelli di IA più avanzati, contribuire a promuovere standard e pratiche di test, con regole comuni in tutti gli Stati membri.

La nuova struttura di governance dell'IA proposta prevede anche l'istituzione del Comitato per l'IA (European Artificial Intelligence Board o EAIB), composto da un rappresentante per ciascuno Stato membro, per svolgere compiti di coordinamento e consultivi per la Commissione e garantire l'armonizzazione tra gli Stati nell'applicazione dell'AI Act.

Viene poi prevista anche l'istituzione di un comitato scientifico di esperti indipendenti, selezionati dalla Commissione europea per fornire consulenza tecnica e contributi all'Ufficio per l'IA. Il comitato scientifico potrà inoltre segnalare all'Ufficio per l'IA eventuali rischi materiali di sicurezza connessi ai modelli di base, contribuire allo sviluppo di strumenti e metodologie per valutare le capacità dei modelli e dei sistemi di IA ad uso generale e fornire consigli sulla classificazione dei modelli di IA ad uso generale con rischi sistemici.

Il Forum consultivo per gli stakeholder, invece, ricomprenderà rappresentanti dell'industria, PMI, start-up, membri della società civile e del mondo accademico e avrà il compito di fornire le competenze tecniche al Comitato per l'IA e alla Commissione, anche attraverso la redazione di opinioni e raccomandazioni.

A livello nazionale, in base al testo dell'AI Act, ogni Stato membro sarà tenuto a istituire autorità nazionali con le competenze ad esse assegnate dal Regolamento. Tali autorità saranno responsabili dell'applicazione delle sanzioni previste in caso di violazioni dell'AI Act. Le autorità nazionali dovranno operare in modo indipendente, imparziale e senza pregiudizi, nonché essere dotate delle risorse necessarie in termini tecnici, finanziari, umani e infrastrutturali per adempiere efficacemente ai loro compiti. Si richiede in particolare che abbiano competenze che comprendano una conoscenza approfondita delle tecnologie dell'intelligenza artificiale, dei dati utilizzati da queste tecnologie, e dei relativi trattamenti attraverso algoritmi, nonché in materia di protezione dei dati personali, della sicurezza informatica e degli standard esistenti. In caso di rispetto di tali requisiti, l'AI Act prevede la possibilità di istituire più autorità, conformemente alle esigenze organizzative dello Stato membro.

8. Le sanzioni

Sul piano sanzionatorio si prevede, infine, che, gli Stati membri stabiliscano sanzioni dettagliate e altre misure di applicazione per la violazione dell'AI Act da parte degli operatori. Le sanzioni previste devono essere efficaci, proporzionate e dissuasive e tenere conto degli interessi delle piccole e medie imprese (PMI), comprese le startup e la loro redditività economica.

Per fare alcuni esempi, in caso di violazioni delle c.d. pratiche vietate le sanzioni possono giungere fino a 35 milioni di euro o al 7% del fatturato mondiale annuo nell'anno precedente, se superiore. In caso di violazione di altri obblighi e requisiti previsti dall'AI Act si prevedono sanzioni che possono giungere fino a 15 milioni di euro o al 3% del fatturato mondiale annuo nell'anno precedente, se superiore. Nel caso, invece, in cui vengano fornite informazioni inesatte, incomplete o fuorvianti alle autorità, la sanzione può giungere fino a 7,5 milioni di euro o all'1% del fatturato mondiale annuo nell'anno precedente, se superiore.

Infine, possono essere imposte ai fornitori di modelli GPAI sanzioni non superiori al 3% del fatturato mondiale totale dell'esercizio finanziario precedente o a 15 milioni di euro, se superiore. Tali sanzioni non dovrebbero essere comminate prima di un anno dall'entrata in vigore delle disposizioni dell'AI Act applicabili, in modo da lasciare ai fornitori di tali sistemi un tempo sufficiente per adeguarsi alla nuova normativa.

Soglie più basse sono però previste in caso in cui la violazione sia commessa da PMI o start-up.

Conclusioni

Dopo l'approvazione del Parlamento del 13 marzo, il testo del Regolamento sarà soggetto a un'ultima revisione da parte dei giuristi-linguisti e dovrà essere adottato definitivamente durante la prossima sessione plenaria del Parlamento Europeo, programmata per il mese di aprile.. L'AI Act dovrà poi ricevere l'approvazione formale dal Consiglio e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea, presumibilmente nel mese di maggio di quest'anno.

L'AI Act entrerà quindi in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale dell'UE e sarà pienamente applicabile dopo 24 mesi. Tuttavia, alcune disposizioni specifiche avranno date di applicazione diverse, come i divieti relativi a sistemi di IA con un livello di rischio inaccettabile, che saranno applicabili a partire da 6 mesi dopo l'entrata in vigore, o le previsioni relative ai modelli GPAI già presenti sul mercato, per i quali è previsto un termine di 12 mesi per garantire la conformità a quanto previsto nel Regolamento.

Le aziende devono quindi iniziare sin da adesso a valutare gli impatti del Regolamento sull'IA sulla propria attività e sui propri prodotti, implementando solide strategie di governance e adottando politiche rigorose per conformarsi alle previsioni del Regolamento, anche al fine di mitigarne i rischi e sfruttare appieno le opportunità che l'AI Act apporterà nel mercato.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it