Maggio 2024

ARTIFICIAL INTELLIGENCE ACT

Breve analisi dei punti salienti dell'AI Act, ossia il regolamento europeo che rappresenta il primo tentativo dell'Unione di fornire una disciplina giuridica dell'utilizzo dell'intelligenza artificiale nel suo complesso

UNISTUDIO LEGAL & TAX
VIA DURINI 26
20122 MILANO
T. +39.02.83418800
VIA DOMINUTTI 20
37135 VERONA
T. +39.045.8013399
VIA DEI TRE OROLOGI 14
00197 ROMA
T. +39.06.73100755
info@unistudio.it
www.unistudio.it
C.F. e P.IVA 02901730230

Tra poche settimane potrebbe finalmente concludersi il primo tentativo dell'Unione Europea di fornire una regolamentazione organica di alcuni profili della disciplina giuridica dell'intelligenza artificiale.

Si allude naturalmente all'*Artificial Intelligence Act*, spesso abbreviato in *AI Act*, il cui testo finale è stato recentemente approvato dal Parlamento Europeo e la cui pubblicazione in Gazzetta Ufficiale è prevista per l'estate 2024.

Il legislatore europeo ha scelto un approccio normativo orizzontale, volto a disciplinare l'intelligenza artificiale nel suo complesso, e non in singoli settori o specifiche materie.

Con riguardo alla definizione di Intelligenza Artificiale, essa si deve intendere, ai fini del Regolamento, come **qualsiasi modello di implementazione basato su una macchina in grado di dedurre dall'*input* che riceve, grazie all'implementazione di sofisticate capacità adattive dotate di diversi livelli di autonomia, una serie di dati processabili finalizzati a generare svariati *output* suscettibili di influenzare ambienti fisici o virtuali.**

Gli scopi che si prefigge l'AI ACT sono i seguenti:
- imporre regole da applicare ai sistemi di AI;
- classificare i dispositivi intelligenti in base al grado di rischio che comportano;
- creare un sistema di *governance* efficace;
- rafforzare la protezione dei diritti che vengono in gioco.

Con riguardo al contenuto, l'*Artificial Intelligence Act* adotta un approccio *risk-based*, che mira alla responsabilizzazione dei soggetti implicati nella catena di produzione, implementazione e distribuzione di sistemi di AI.
Si tratta di un modello che tenta di arretrare la linea della responsabilità dei soggetti, i quali sono chiamati – in diversa misura – a adottare, *ex ante*, misure che mitighino il rischio connesso all'utilizzo di questi sistemi e a essere così *compliant* con quanto richiesto dal legislatore.

Il sistema di gestione del rischio è suddiviso in cinque fasi principali: l'**identificazione** del rischio; la sua **analisi**, per valutarne impatto e probabilità; la **valutazione** in merito a come trattare il rischio; l'eventuale azione di **trattamento** del rischio e infine il **monitoraggio** dello stesso.
Maggiore è il rischio insito nell'utilizzo di un determinato sistema intelligenza artificiale e più ampie saranno, conseguentemente, le responsabilità di chi sviluppa, implementa e utilizza quel sistema, sino a giungere a un divieto di utilizzo delle applicazioni e delle tecnologie il cui rischio è considerato inaccettabile (come prevede l'art. 5).
A differenza di quanto accade nel GDPR, il rischio nell'*AI Act* è predeterminato: è quindi il legislatore stesso a classificare i diversi sistemi di AI entro determinate categorie e imporre conseguenti obblighi di *accountability*.

In particolare, vi sono modelli di intelligenza artificiale vietati, in quanto il rischio è considerato inaccettabile. Tali modelli non possono essere commercializzati né utilizzati dalle pubbliche autorità se non per scopi specifici.
Tra questi si annoverano i sistemi che sfruttano **tecnologie subliminali per manipolare i comportamenti** di una persona; quelli che abusano di persone vulnerabili e fragili; modelli volti a **categorizzare** le persone fisiche in base ai loro dati biometrici per dedurne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, o l'orientamento sessuale. Questi ultimi sistemi possono essere utilizzati per fini di sicurezza pubblica, ma esclusivamente nel caso di ricerca di vittime di rapimento, tratta di esseri umani o persone scomparse, o per prevenire una minaccia di un attacco terroristico.

Sono vietati poi i sistemi di cd. *social scoring* per la valutazione o la classificazione di persone fisiche o di gruppi di essi.
Altri sistemi vietati sono quelli d**i polizia predittiva**, che sfruttano gli algoritmi per prevedere le probabilità con cui può essere commesso un reato e tutte le informazioni a esso legato.

Proibiti sono altresì i sistemi AI che svelano le emozioni delle persone sul posto di lavoro o nelle istituzioni scolastiche, ad eccezione in cui tali sistemi non vengano utilizzati per motivi medici o di sicurezza.
Nell'ambito produttivo saranno quindi vietati gli utilizzi di strumenti di sorveglianza in tempo reale dei dipendenti, ma anche i cd. software di *affective computing*, ossia quelle applicazioni volte a leggere le nostre emozioni per sfruttarle.

Nell'ambito dei casi in cui l'utilizzo dell'AI è concesso, grande attenzione viene offerta ai sistemi ad alto rischio, individuati all'art. 6 dell'*AI Act*.
Per identificare i sistemi di intelligenza artificiale ad alto rischio, l'*AI Act* fa riferimento ai **diritti fondamentali dell'uomo**.
Per alto rischio, quei sistemi che possono porre rischi significativi per la salute e la sicurezza, per i diritti fondamentali delle persone, la democrazia, lo Stato di diritto e le libertà individuali.
Consistono nello specifico in:

- sistemi di AI destinati a essere utilizzati come componenti di sicurezza di prodotti (o qualora i sistemi di AI siano essi stessi prodotti);
- sistemi di AI che rientrano in uno o più settori critici, se presentano un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche

Questi sistemi saranno sottoposti obbligatoriamente a una valutazione di conformità preventiva **di identificazione e analisi dei rischi noti, possibili e prevedibili** con conseguenze sulla salute, sulla sicurezza e sui diritti fondamentali degli individui.

Dovranno, inoltre, essere addestrati e testati con set di dati sufficientemente rappresentativi per ridurre al minimo il rischio di integrare distorsioni inique nel modello. Dovranno anche essere tracciabili e verificabili, garantendo la conservazione dell'opportuna documentazione, compresi i dati utilizzati per addestrare l'algoritmo, fondamentali per le indagini *ex post*.

Questi modelli dovranno anche essere sottoposti a una valutazione di impatto sui diritti fondamentali.

Relativamente a questo approccio al rischio, l'*AI Act* specifica anche che il processo di gestione dei rischi deve essere eseguito durante tutto il **ciclo di vita** del sistema di AI, monitorato sistematicamente e aggiornato, qualora emergano nuovi rischi.
Per rendere effettivo il sistema, i soggetti chiamati a questo processo sono molteplici, nei loro diversi ruoli: il produttore, il fornitore, l'implementatore, l'importatore etc.

In fase di implementazione di questo regolamento gli operatori dovranno affrontare diversi aspetti problematici.

In particolare, GDPR e *AI Act* sono due regolamenti fortemente complementari, se non parzialmente sovrapponibili tra loro: il dato è la minima unità strutturale dell'AI, pertanto i due regolamenti devono essere coordinati. Eppure, presentano vari punti di divergenza.

Fondamentalmente, i regolamenti rappresentano espressioni molto diverse della logica di approccio al rischio: il GDPR segue una prospettiva di *bottom up*, in base a cui le misure di mitigazione sono rimesse alla piena discrezionalità del titolare del trattamento, che viene pienamente responsabilizzato, e non definite dalla legge; nell'*AI Act*, invece, si segue una logica contraria, ossia di *top down*, per la quale è il legislatore a prevedere distinti livelli di rischio e connessi gradi di responsabilità.

La differente prospettiva adottata dai due regolamenti imporrà agli operatori un bilanciamento necessario tra i due modelli.

Tale regolamento rappresenta senz'altro il primo passo nella regolamentazione giuridica dell'AI, nel tentativo di coniugare il progresso tecnologico con le esigenze di certezza del diritto.