Novità normativa

INTELLIGENZA ARTIFICIALE: GLI OBBLIGHI IN CAPO A TUTTE LE IMPRESE IN VIGORE DAL 2 FEBBRAIO 2025

Il 12 luglio 2024 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento UE 2024/1689, noto a tutti come *Artificial Intelligence Act* (**AI Act**), il quale stabilisce *regole armonizzate sull'intelligenza artificiale*.
Il Regolamento, direttamente applicabile in tutti gli Stati membri, mira a supportare la diffusione delle tecnologie di IA, garantendo al contempo un livello uniforme di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali.

"***Propongo di considerare una domanda: le macchine possono pensare***?"[1], se lo chiedeva Alan Turing a metà del 1900 ed è l'interrogativo che almeno una volta ciascuno di noi si è posto nel corso degli ultimi mesi.
I sistemi informatici intelligenti trovano, infatti, sempre maggiore applicazione nei settori più eterogenei: dalla medicina al commercio, dai mercati azionari ai trasporti, dall'industria ai sistemi di informazione e comunicazione, contribuendo a migliorare efficienza ed innovazione in ogni campo.
Secondo Goldman Sachs, l'intelligenza artificiale potrebbe essere associata a una maggiore crescita del PIL dei Paesi sviluppati di quasi mezzo punto percentuale all'anno nella prossima decade; McKinsey stima che sull'intelligenza artificiale si giocheranno tra i 4 e i 6 trilioni di maggiore prodotto interno lordo globale[2].
La questione, insomma, è strategica e dipende anche e soprattutto dalla **capacità delle imprese di cogliere le opportunità**, rappresentando l'IA uno strumento fondamentale per l'efficientamento dei processi, considerato che si stima che l'AI possa incrementare la produttività aziendale con una crescita prospettata tra il 5% e il 20%, contribuendo anche ad affrontare la mancanza di manodopera legata alla diminuzione della popolazione. Si tratta quindi di un'opportunità che le imprese italiane, incluse le PMI, dovranno cogliere per mantenere la propria competitività a livello internazionale[3].
Nell'attuale contesto geopolitico, che vede Cina e Stati Uniti come principali *player* del settore, l'Europa, con l'*AI Act*, si pone come *leader* nella produzione normativa, trattandosi del primo testo organico a livello mondiale, con cui l'Europa si propone di *affermare una "sovranità digitale" europea che è insieme esterna, verso gli altri due principali attori globali, e interna, verso gli Stati nazionali europei. Da un lato si vuole affermare un nuovo modello e, dall'altro, evitare la frammentazione interna*[4].
Con l'*AI Act*, l'Unione europea ha scelto un approccio regolatorio orizzontale: questo significa che l'intelligenza artificiale viene regolamentata in via generale e non, invece, disciplinando applicazioni specifiche della stessa.

Ma cos'è l'intelligenza artificiale?

Ai sensi dell'*AI Act*, un sistema di IA è "*un sistema automatizzato progettato per funzionare con livelli*

[1] Alan Turing, *Computing Machinery and Intelligence*, 1950.
[2] R. Viola, L. De Biase, *La legge dell'intelligenza artificiale*, Il Sole 24 Ore Tecnologia, n. 1/24.
[3] Il Sole 24 Ore, *L'Intelligenza Artificiale per aumentare la produttività aziendale*, Newsletter.
[4] Così, G. Finocchiaro, *Intelligenza artificiale. Quali regole?,* Il Mulino, p. 109.

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".
La definizione, come si vede, è estremamente generale, ma ciò è coerente con il succitato approccio regolamentare e risponde anche all'esigenza di contenere in sé i rapidi sviluppi tecnologici in questo ambito, come si legge nel Considerando n. 12 del Regolamento stesso.

A chi si applica l'AI Act?
Il Regolamento si applica **ai soggetti pubblici e privati**, all'interno e all'esterno dell'UE, a condizione che il sistema di IA sia immesso sul mercato dell'Unione o che il suo uso abbia effetti su persone situate nell'UE.
L'AI Act, disciplina i sistemi di IA seguendo un **approccio basato sul rischio**, in base al quale il rigore delle regole che devono essere adottate è tanto maggiore quanto più è elevato il rischio, dove per "rischio" si intende la **probabilità** e la **gravità** dell'impatto negativo che un sistema di IA potrebbe avere sui diritti fondamentali.

Quali nuovi obblighi impone la normativa europea?
L'*AI Act* prevede regole diverse, nonché differenti obblighi per fornitori e utenti, a seconda che il **livello di rischio** derivante dal sistema IA sia:

i. inaccettabile
ii. alto
iii. basso o minimo
iv. limitato.

I sistemi di IA che determinano un rischio considerato **inaccettabile** sono vietati ai sensi dell'art. 5 del Regolamento.
In questa categoria rientrano i sistemi che possono manipolare il comportamento umano, come quelli che consentono di attribuire un "punteggio sociale" (cd. *social scoring*), per finalità pubbliche e private, classificando le persone in base al loro comportamento sociale o alle loro caratteristiche personali.
Per i sistemi di IA ad **alto rischio**, è previsto il rispetto di stringenti requisiti, oltre ad una valutazione di conformità di tali requisiti prima della messa in commercio e, in seguito, un costante monitoraggio.
L'elenco delle tecnologie rientranti in questa categoria è contenuto nell'Allegato III del Regolamento e ricomprende i sistemi di IA:
• di identificazione biometrica remota, categorizzazione *biometrica* e riconoscimento delle emozioni (al di fuori delle categorie vietate);
• utilizzati come componenti di *sicurezza* nella gestione e nel funzionamento delle *infrastrutture digitali critiche*, del traffico stradale e della fornitura di acqua, gas, riscaldamento ed elettricità;
• finalizzati a determinare l'accesso, l'ammissione o l'assegnazione agli istituti di istruzione e *formazione* professionale (ad esempio, per valutare i risultati dell'apprendimento e orientare il processo di apprendimento e il monitoraggio dei comportamenti disonesti);
• relativi alla valutazione dell'occupazione, ad ottimizzare la gestione dei lavoratori e l'accesso al *lavoro* autonomo (ad esempio, per pubblicare annunci di lavoro mirati, analizzare e filtrare le candidature e valutare i candidati);
• usati per determinare l'accesso a servizi e a prestazioni pubblici e privati essenziali (come, ad esempio, l'assistenza *sanitaria*);
• finalizzati alla *valutazione dell'affidabilità creditizia* delle persone fisiche, alla valutazione dei rischi finanziari, nonché alla determinazione dei prezzi in relazione ad assicurazioni sulla vita e assicurazioni sanitarie;
• utilizzati nelle attività di contrasto, di gestione della *migrazione*, dell'asilo e del controllo delle frontiere, di amministrazione della giustizia, nonché nello svolgimento dei processi democratici e per la valutazione e classificazione delle chiamate di emergenza.
I sistemi di IA a **rischio minimo**, come videogiochi o filtri spam, sono esenti da obblighi, con la

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

possibilità, caldeggiata, di aderire volontariamente a codici di condotta.
Infine, per i sistemi considerati a **rischio limitato** il capo IV del Regolamento prevede specifici obblighi di trasparenza in capo ai soggetti coinvolti nell'implementazione e nell'utilizzo di tali sistemi di IA, imponendo che l'informativa venga data in maniera chiara e distinguibile al più tardi al momento della prima interazione.

Quindi, che cosa devono fare le imprese?
La risposta a questo interrogativo apre le porte ad all'analisi di un'altra questione che il Regolamento affronta, e cioè la suddivisione dei vari soggetti coinvolti in categorie, cui ricondurre – in considerazione dello specifico ruolo svolto – una serie di obblighi e di adempimenti.
Per quanto riguarda **i fornitori di sistemi di IA ad alto rischio** – ovvero *coloro che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli si IA per finalità generali dell'Unione* (art. 3 del Regolamento) – l'art. 9 del Regolamento impone anzitutto che venga ***istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi***, che ai sensi dell'art. 9, par. 2, del Regolamento, viene definito come "*un processo iterativo continuo eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un aggiornamento costante e sistematico*".
Occorre, cioè, porre in essere una serie di attività che consentano di **identificare**, **stimare** e **valutare** i rischi (noti e prevedibili) che possono derivare dall'utilizzo del sistema, sia quando usato conformemente alla sua finalità, sia quando utilizzato in maniera impropria, ma ragionevolmente prevedibile.
Una volta conclusa tale complessa operazione, devono essere adottate **adeguate misure di gestione**, le quali devono far sì che il **rischio residuo** associato a ciascun pericolo, nonché il **rischio residuo complessivo**, siano considerati accettabili in relazione ad un utilizzo del sistema IA ad alto rischio conforme alla sua finalità prevista o ad un uso improprio ragionevolmente prevedibile (art 9, par. 4).

Il Regolamento prevede, poi, una disciplina specifica concernente la **qualità e la governance dei dati di addestramento**, convalida e prova (art. 10); l'obbligo di redigere la documentazione tecnica di un sistema di IA ad alto rischio che consenta di poterne verificare la conformità (art. 11); che il sistema sia tale da garantire agli utenti di *interpretare l'output del sistema e utilizzarlo adeguatamente* (art. 13); la progettazione e sviluppo dei sistemi di IA ad alto rischio in modo tale che possano essere efficacemente supervisionati da persone fisiche durante il loro utilizzo (art. 14).
Per quanto riguarda i **deployer di sistemi di IA ad alto rischio** – ovvero *le persone fisiche o giuridiche, le autorità pubbliche o altri organismi che utilizzano 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* (art. 3 del Regolamento) – l'art. 26 del Regolamento prevede che adottino **idonee misure tecniche e organizzative per garantire l'utilizzo tali sistemi in maniera conforme**.
I deployer, inoltre, devono affidare la *sorveglianza umana* a persone fisiche che dispongono della competenza, della formazione e dell'autorità a ciò necessarie.
L'AI Act prevede, inoltre, all'art. 50 una nutrita serie di obblighi cui sono soggetti **tanto i fornitori quanto i deployers di determinati sistemi di IA**. In particolare, i fornitori di sistemi di IA progettati per dialogare direttamente con persone fisiche devono assicurarsi che queste siano consapevoli di stare interagendo con un sistema di IA, con la sola eccezione relativa ai sistemi di IA autorizzati per legge ad accertare, prevenire o perseguire crimini. I fornitori di sistemi di IA, inclusi quelli progettati per scopi generali che producono contenuti sintetici audio, visivi, video o testuali, sono tenuti a garantire che questi *output* siano chiaramente identificabili come generati artificialmente e devono assicurarsi, altresì, che le soluzioni tecniche proposte per questa marcatura siano efficaci, interoperabili, robuste e affidabili.

Viale San Francesco d'Assisi, 8
38122 TRENTO
T. +39 0461 231000 | 260200 | 261977
F. +39 0461 269518
studio@slm.tn.it
www.slm.tn.it

In un tale contesto normativo, dunque, è imprescindibile per le realtà aziendali che vogliano sfruttare il potenziale dell'Intelligenza Artificiale, l'**adozione di un'AI policy** e ciò, invero, anche a prescindere dagli specifici obblighi contenuti nella normativa appena analizzata.

È innegabile, infatti, che l'IA è già entrata nelle aziende e che sono in crescita esponenziale i soggetti che vi fanno ricorso nello svolgimento della propria attività lavorativa. Nessuna organizzazione può permettersi il rischio di un utilizzo incontrollato dei sistemi di IA per mancanza di regole interne.

Il pericolo di violazione della normativa in tema di tutela dei dati personali e sul diritto d'autore, il rischio di condivisione di dati che l'impresa ha interesse a mantenere riservati e la necessità di verificare affidabilità e qualità degli output sono solo alcuni dei rischi concreti cui quotidianamente le organizzazioni sono già esposte e che la policy relativa all'utilizzo dell'intelligenza artificiale dovrà disciplinare.

L'*AI Act* è entrato in vigore il 1° agosto 2024, ma dovrà trovare effettiva attuazione in tutte le sue parti a decorrere dal 2 agosto 2026, anche se già a partire dal 2 febbraio 2025 dovranno trovare applicazione le disposizioni concernenti le pratiche di IA vietate.

È indubbio, tuttavia, che la **rivoluzione tecnologica e culturale** che ruota attorno all'intelligenza artificiale è già nel pieno del suo svolgimento e che, nonostante il periodo di transizione previsto per la completa applicabilità della normativa cogente, già oggi nessuna realtà imprenditoriale può progettare o acquistare soluzioni di IA senza averne prima verificato la compatibilità con le norme contenute nell'AI Act, correndo il rischio che, dopo soli due anni, tali tecnologie divengano inutilizzabili.

ULTERIORI INFORMAZIONI SU QUESTO ARGOMENTO O SU FATTISPECIE CORRELATE POSSONO ESSERE RICHIESTE A:

avv. Selene Sontacchi
+39 0461 23100 – 260200 - 261977
ss@slm.tn.it