MEMO

Regolamento (UE) 2024/1689

AI ACT

Sistema di Intelligenza Artificiale

Il **Regolamento (UE) 2024/1689** (di seguito, il **Regolamento** o l'**AI Act**) definisce un **sistema di Intelligenza Artificiale** come *"un sistema automatizzato progettato per funzionare con livelli 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"*.

Soggetti rilevanti

L'AI Act individua una serie di **figure destinatarie della normativa**. Tra queste, le più importanti sono:

a) **Fornitore:** 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;

b) **Deployer:** una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un 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;

c) **Rappresentante autorizzato:** una persona fisica o giuridica ubicata o stabilita nell'Unione che ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA o di un modello di IA per finalità generali al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal Regolamento;

d) **Importatore:** una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo;

e) **Distributore:** una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione.

Classificazione dei sistemi di Intelligenza Artificiale

L'AI Act adotta un **approccio basato sul rischio**: più sono **elevati i rischi** che l'utilizzo degli strumenti basati sull'intelligenza artificiale comportano, più devono essere **stringenti le misure** predisposte per ridurre al minimo i rischi per la salute, la sicurezza ed i diritti fondamentali delle persone. In particolare, viene individuato un:

a) **Rischio inaccettabile**: vi rientrano i sistemi o applicazioni di IA che influenzano in maniera significativa gli utenti, distorcendone il comportamento, mediante tecniche manipolative, ingannevoli o sfruttandone le vulnerabilità (ad esempio, i giocattoli che utilizzano l'assistenza vocale incoraggiando comportamenti pericolosi dei minori), i sistemi che consentono il "social scoring" da parte di governi o aziende, o finalizzati alla profilazione a fini predittivi di comportamenti illeciti o, ancora, i sistemi di categorizzazione ed identificazione biometrica privi delle opportune garanzie proprie di una società democratica. Pratiche di IA di tal genere possono implicare una lesione dei diritti fondamentali delle persone e, di conseguenza, saranno **vietati all'interno della UE**. Ad esempio, **non sarà consentito** utilizzare sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso di tale sistema sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza.

b) **Alto rischio**: alcuni sistemi di IA, identificati dall'AI Act in appositi Allegati, che potranno comportare delle conseguenze sulla salute, sulla sicurezza o sui diritti fondamentali delle persone, per essere ammessi all'interno dell'UE, dovranno soddisfare **requisiti rigorosi**, specificati nel successivo paragrafo. I sistemi per determinare l'accesso ad istituti di istruzione o per il reclutamento di personale o i sistemi di identificazione biometrica remota, categorizzazione biometrica in basa ad attributi o caratterestiche sensibili e di riconoscimento delle emozioni costituiscono esempi di sistemi di IA ad alto rischio.

c) **Rischio di trasparenza**: alcuni sistemi di IA destinati ad interagire direttamente con le persone fisiche, o che generano o manipolano immagini, contenuti, audio o video, possono comportare **specifici rischi** di furti di identità, manipolazioni o inganni (ad esempio, i

chatbots o i c.d. *deep fakes*). A tale riguardo, sono previsti specifici obblighi di informazione e trasparenza. In particolare: *(i)* quando si utilizzeranno tali sistemi di intelligenza artificiale sarà necessario rendere gli utenti consapevoli del fatto che la loro interazione avviene con una macchina; *(ii)* i contenuti generati dall'intelligenza artificiale (ad esempio, i *deep fakes*) dovranno essere espressamente segnalati; *(iii)* nella progettazione di sistemi di IA, il contenuto sintetico di audio, video, testo e immagini dovrà essere contrassegnato in un formato leggibile dalla macchina e riconoscibile come generato o manipolato artificialmente.

d) **Rischio minimo**: si tratta dei sistemi che presentano **rischi minimi o nulli** per i diritti e/o la sicurezza dei cittadini (ad esempio, i sistemi di raccomandazione abilitati dall'IA, i filtri antispam, ecc.). Tali sistemi beneficeranno dell'assenza di obblighi specifici; ad ogni modo, relativamente all'uso di questi sistemi di IA, potranno essere introdotti dei codici di buone pratiche a cui le aziende potranno volontariamente aderire.

Sistemi di Intelligenza Artificiale ad alto rischio

Definizione

In primo luogo, un sistema di IA si definisce **ad alto rischio** se sono **soddisfatte entrambe le condizioni seguenti**:

a) il sistema di IA è destinato ad essere **utilizzato come componente di sicurezza** di un prodotto, o il sistema di IA è **esso stesso un prodotto**, **disciplinato dalla normativa di armonizzazione dell'Unione** elencata nell'Allegato I dell'AI Act;

b) il prodotto, il cui componente di sicurezza a norma della lett. a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una **valutazione della conformità** da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'Allegato I.

Oltre ai sistemi di IA ad alto rischio di cui sopra, sono **considerati ad alto rischio** anche i sistemi di IA di cui all'**Allegato III** dell'AI Act.

In particolare, i **settori individuati** come ad alto rischio riguardano: *(i)* la biometria; *(ii)* le infrastrutture critiche (digitali, traffico stradale, forniture essenziali); *(iii)* l'istruzione e la formazione professionale; *(iv)* l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo; *(v)* i servizi privati e pubblici essenziali; *(vi)* l'attività di contrasto di condotte criminose; *(vii)* la migrazione, l'asilo e la gestone del controllo delle frontiere; nonché *(viii)* l'amministrazione della giustizia e processi democratici.

Tuttavia, un sistema di IA di cui all'Allegato III **non è considerato ad alto rischio** se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale.

Fatto salvo quanto sopra, un sistema di IA di cui all'Allegato III **è sempre considerato** ad alto rischio qualora esso effettui **profilazione** di persone fisiche.

Adempimenti

Tenendo conto delle previste **finalità** nonché dello **stato dell'arte** generalmente riconosciuto in materia di IA e di tecnologie correlate all'IA, in relazione ai **sistemi di IA considerati ad alto rischio** vengono previsti in particolare **obblighi di**:

a) istituire, attuare, documentare e mantenere un sistema di gestione dei rischi, inteso come un processo iterativo, continuo, pianificato ed eseguito nel corso dell'intero ciclo di vita del sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici (**sistema di gestione dei rischi**);

b) in caso di impiego di tecniche che prevedono l'uso di dati per l'addestramento di modelli di IA, utilizzare **set di dati di addestramento, convalida e prova** che soddisfino i criteri di qualità e liceità stabiliti dal Regolamento;

c) redigere, prima dell'immissione sul mercato o della messa in servizio (e tenere successivamente aggiornata), una **documentazione tecnica** idonea a dimostrare che il sistema di IA ad alto rischio sia conforme ai requisiti previsti nel Regolamento;

d) consentire, a livello tecnico, la **registrazione automatica degli eventi** (c.d. "**log**") per la durata del ciclo di vita del sistema.

I sistemi di IA considerati ad alto rischio dovranno inoltre **essere progettati e sviluppati**:

a) in modo tale da garantire che il loro funzionamento sia sufficientemente **trasparente** per consentire ai deployer (vale a dire, a chiunque utilizzi un sistema di IA sotto la propria autorità, ad eccezione del caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale) di interpretare l'output del sistema e di utilizzarlo adeguatamente;

b) per poter essere efficacemente **supervisionati da persone fisiche** durante il periodo in cui sono in uso;

c) al fine di conseguire un adeguato **livello di accuratezza, robustezza e cybersicurezza** e di operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita.

Inoltre, occorre tenere presente che, **prima** di utilizzare un sistema di IA ad alto rischio, i deployer che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i deployer di alcuni specifici sistemi di IA ad alto rischio (Allegato III, punto 5, lett. b) e c) saranno tenuti ad effettuare una **valutazione dell'impatto sui diritti fondamentali** che l'uso di tale sistema può produrre (c.d. *Fundamental Rights Impact Assessment*). Tale valutazione dovrà comprendere almeno i **seguenti elementi**: *(i)* una descrizione dei processi del *deployer* in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista; *(ii)* una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; *(iii)* le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; *(iv)* i rischi specifici di danno che possono incidere su determinate categorie di persone fisiche o su certi gruppi di persone; *(v)* una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; *(vi)* le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.

Modelli di Intelligenza Artificiale per finalità generali

Prescrizioni generali

L'AI Act prevede altresì norme specifiche per i **modelli di Intelligenza Artificiale a finalità generali**, definiti come quei modelli di IA che, anche laddove addestrati con grandi quantità di dati utilizzando l'auto-supervisione su larga scala, siano *(i)* caratterizzati da una **generalità significativa**, *(ii)* in grado di svolgere con competenza un'**ampia gamma di compiti distinti**, indipendentemente dalle modalità con cui il modello è immesso sul mercato e *(iii)* possano essere **integrati in una varietà di sistemi o applicazioni** a valle.

A tal proposito, tra gli altri, in capo ai fornitori di modelli di IA per finalità generali vengono previsti specifici **requisiti di trasparenza**, tra cui l'onere di:

a) redigere e mantenere una **documentazione tecnica aggiornata** e rendere disponibili informazioni e documentazione ai fornitori di sistemi di IA che intendono integrare il modello di IA per finalità generali nei loro sistemi di IA;

b) mettere in atto una **politica volta a tutelare il diritto d'autore**, anche attraverso l'impiego di tecnologie all'avanguardia (ad esempio, utilizzando tecnologie di *watermarking*);

c) redigere e rendere pubblica una **sintesi dei contenuti utilizzati per l'addestramento dei modelli**, secondo un template che verrà reso disponibile dall'Ufficio per l'IA;

d) in caso di stabilimento al di fuori dell'UE, nominare un **rappresentante autorizzato** nell'Unione Europea.

Verranno **esentati** dall'adempimento di alcuni degli obblighi sopra menzionati solo i fornitori di modelli di IA rilasciati con **licenza libera e *open source*** (ad esempio, dagli obblighi relativi alla divulgazione della documentazione tecnica), considerati gli effetti positivi sulla ricerca, l'innovazione e la concorrenza che modelli di tal genere possono comportare. Ad ogni modo, anche se *open source*, **non saranno esentati** alcuni modelli di IA per finalità generali che pongono rischi sistemici.

Obblighi per i modelli di IA per finalità generali con rischio sistemico

Sono modelli di IA per finalità generali con rischio sistemico i modelli che potrebbero avere un **impatto significativo** sul mercato interno a causa della loro portata e dei loro effetti negativi reali o ragionevolmente prevedibili (ad esempio, sulla salute pubblica, sulla sicurezza, sulla pubblica sicurezza, sui diritti fondamentali o sulla società nel suo complesso).
Oltre ai requisiti di trasparenza e protezione del diritto d'autore altrui che gravano su tutti i modelli di IA per finalità generali, i fornitori di modelli di IA per finalità generali a rischio sistemico sono tenuti, in particolare, a **valutare e mitigare costantemente i rischi** che essi comportano anche garantendo un adeguato **livello adeguato di cybersicurezza**.

Codici di buone pratiche e presunzione di conformità

I fornitori di modelli IA per finalità generali potranno fare affidamento su codici di buone pratiche per **dimostrare la conformità** con gli obblighi stabiliti dall'AI Act.
A tale proposito, la Commissione potrà decidere di **approvare un codice di buone pratiche** e conferirgli validità generale all'interno dell'Unione europea o, in alternativa, di **fornire norme comuni** per l'attuazione degli obblighi più rilevanti. La conformità a uno standard europeo armonizzato conferirà ai fornitori di modelli di IA per finalità generali una **presunzione di conformità**.

Governance

L'**attuazione dell'AI Act** sarà di competenza di una serie di attori. In particolare:

A livello nazionale, gli Stati membri dovranno istituire o designare almeno *(i)* un'**Autorità di vigilanza del mercato** e *(ii)* un'**Autorità di notifica** per garantire l'applicazione e l'attuazione dell'AI Act.

A livello europeo, al fine di garantire una corretta applicazione, vengono istituiti diversi organi:

a) un **Ufficio per l'IA** all'interno della Commissione per far rispettare le norme comuni in tutta l'Unione;

b) un **Gruppo scientifico di esperti** indipendenti per sostenere le attività di applicazione delle norme;

c) un **Comitato per l'IA**, composto da rappresentanti degli Stati membri, per consigliare e assistere la Commissione e gli Stati membri nell'applicazione coerente ed efficace del Regolamento;

d) un **Forum consultivo** per le parti interessate che fornisca competenze tecniche al Comitato per l'IA e alla Commissione.

Sanzioni

Le **sanzioni** per le violazioni dell'AI Act verranno stabilite:

a) in una **percentuale del fatturato globale annuo** della Società che commetterà la violazione; ovvero

b) in un **importo predeterminato** (a seconda di quale sia il valore più elevato).

In particolare, verranno previste sanzioni fino a **35 milioni di euro** o fino al **7%** del fatturato globale annuo dell'esercizio precedente per le violazioni di pratiche vietate o per la non conformità rispetto a determinate prescrizioni dell'AI Act.
Le **piccole e medie imprese** e le **start-up** saranno invece soggette a sanzioni **proporzionali**.

Timeline

L'AI Act è stato pubblicato il **12 luglio 2024** nella Gazzetta Ufficiale dell'Unione europea ed **entrerà in vigore** dal ventesimo giorno successivo a tale pubblicazione.
Dal **2 agosto 2026** l'intero Regolamento diventerà invece **applicabile**, **ad eccezione**:

- dei divieti relativi a **pratiche di intelligenza artificiale proibite** (rischio inaccettabile), che troveranno applicazione dal **2 febbraio 2025**;
- dei **codici di buone pratiche**, che dovranno essere pronti dal **2 maggio 2025**;
- delle prescrizioni relative ai **sistemi di IA per finalità generali**, che troveranno applicazione dal **2 agosto 2025**;

- degli adempimenti per i **sistemi di IA ad alto rischio**, che troveranno applicazione: *(i)* dal **2 agosto 2026**, nel caso di sistema di IA ad alto rischio che rientri all'interno dell'Allegato III; oppure *(ii)* dal **2 agosto 2027**, nel caso in cui tali sistemi di IA ad alto rischio rientrino nell'elenco della normativa di armonizzazione dell'Unione presente all'interno dell'Allegato I.

Scadenze diversificate saranno, invece, applicate per *(i)* i sistemi e i modelli di IA **già immessi** sul mercato o in servizio e per *(ii)* i modelli di IA per finalità generali **già immessi** sul mercato.

Because we care

ITALIA

Roma
Via Principessa Clotilde, 7
00196 (RM)
T +39 06 36227.1
F +39 06 3235161
mail@tonucci.com

Milano
Via Gonzaga, 5
20123 (MI)
T +39 0285919.1
F +39 02860468
milano@tonucci.com

Padova
Via Trieste, 31/A
35121 (PD)
T +39 049 658655
F +39 049 8787993
padova@tonucci.com

Prato
Via Giuseppe Valentini, 8/A
59100 (PO)
T +39 0574 29269
F +39 0574 604045
prato@tonucci.com

Trieste
Via Del Coroneo, 33
34133 (TS)
T +39 040 366419
F +39 040 0640348
trieste@tonucci.com

Foggia
Via Vincenzo Lanza, 14
71121 (FG)
T +39 0881 707825
F +39 0881 567974
foggia@tonucci.com

ALBANIA

Tirana
Torre Drin - Rruga Abdi Toptani
1001 (TR)
T +355 (0) 4 2250711/2
F +355 (0) 4 2250713
tirana@tonucci.com

ROMANIA

Bucharest
Clădirea Domus II
Str. Știrbei Vodă nr. 114-116
Etaj 2, Sector 1
010119 București
T +40 31 4254030/1/2
F +40 31 4254033
bucharest@tonucci.com