FIVERS

# Il Regolamento 2024/1689 dell'Unione Europea sull'Intelligenza Artificiale in pillole

**MEMORANDUM**

## INDICE

## Quando è stato pubblicato il Regolamento dell'Unione europea sull'Intelligenza Artificiale?

Il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea del 12 Luglio 2024.

Rappresenta la prima legge organica e completa al mondo per la disciplina dell'Intelligenza Artificiale e mira ad affrontare i rischi per la salute, la sicurezza e i diritti fondamentali. Inoltre, il Regolamento 2024/1689 tutela la democrazia, lo Stato di diritto e l'ambiente.

## Quando entra in vigore il Regolamento 2024/1689 (AI Act)?

Il Regolamento 2024/1689 entra in vigore il 1° agosto 2024.

## Quando saranno materialmente applicabili le disposizioni e gli obblighi del Regolamento 2024/1689 (AI Act)?

Il Regolamento 2024/1689 sarà applicabile solo dal 2 agosto 2026. Alcune norme si applicheranno tuttavia dopo 6 o 12 mesi.

Saranno applicabili dal 2 febbraio 2025:

(a) gli articoli da 1 a 4, relativi a oggetto, ambito di applicazione, definizioni (i contratti di fornitura potranno dunque impiegare definizioni tecniche e giuridiche dell'AI Act) e obblighi di alfabetizzazione IA (obbligo per i fornitori e gli sviluppatori di avere personale addestrato e competente, che potrà trovare specifico ingresso nella contrattualistica con i fornitori).
(b) l'art. 5 sulle pratiche di IA vietate (particolare attenzione dovrà essere prestata – ad esempio - alle profilazioni avanzate che utilizzano la biometria, soprattutto sui luoghi di lavoro, per verificare l'applicabilità del divieto).

Dopo 12 mesi (dal 2 agosto 2025) si applicheranno:

(a) le norme sull'impianto sanzionatorio (con sanzioni fino a 35 milioni di euro o al 7% del fatturato globale annuo; la sanzione per i fornitori di modelli IA a scopi generali – fino a 15 milioni di euro o fino al 3% del fatturato – si applicherà dopo 24 mesi);
(b) le norme sui modelli di IA per finalità generali – GPAI (tematica di *compliance* e contrattuale, alla luce di svariati modelli – come Chat-GPT e l'IA generativa – già oggi integrati in soluzioni di ampio utilizzo quotidiano);
(c) le norme sulle Autorità di notifica, sulle relative procedure di notifica e sugli organismi notificati;

(d) l'art. 78 *("Riservatezza dei dati trattati in conformità al Regolamento*");
(e) le norme che istituiscono la banca dati UE sui sistemi di IA ad alto rischio.

Infine, è rinviata al 2 agosto 2027 l'applicabilità delle norme sui sistemi di IA "ad alto rischio", così come dei connessi obblighi.

## A chi si applica il Regolamento 2024/1689?

Il Regolamento 2024/1689 si applicherà 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 utilizzo abbia effetti su persone situate nell'UE.

Le norme vincoleranno sia i fornitori/sviluppatori di sistemi IA (ad esempio uno sviluppatore di uno strumento di screening dei CV) quanto gli utilizzatori professionali finali (detti "*deployer*") di sistemi di IA ad alto rischio (ad esempio, un'azienda che acquista il suddetto strumento di screening).

Il Regolamento 2024/1689 si applicherà inoltre a tutta la filiera commerciale (importatori, distributori, fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio, etc): gli importatori di sistemi di IA nella UE dovranno ad esempio garantire che il fornitore extra-UE abbia già eseguito l'appropriata procedura di valutazione della conformità e che il sistema IA rechi una marcatura di conformità europea (CE) e sia corredato della documentazione e delle istruzioni per l'uso richieste.

Sono inoltre previsti specifici obblighi per i fornitori di modelli di IA per finalità generali (detti GPAI) compresi i modelli di IA generativa di grandi dimensioni (i sistemi LLM – Large Language Models, come Chat-GPT, Copilot, Gemini, etc).

I fornitori di modelli gratuiti e open source sono esentati dalla maggior parte di questi obblighi. Tale esenzione non riguarda tuttavia gli obblighi applicabili ai fornitori di modelli di IA per finalità generali GPAI che comportano rischi sistemici.

Il Regolamento 2024/1689 non si applicherà alle attività di ricerca, sviluppo e prototipazione che precedono l'immissione sul mercato e ai sistemi di IA sviluppati per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

## In che senso il Regolamento 2024/1689 disciplina l'Intelligenza Artificiale in base alla tipologia di rischio (approccio risk-based)?

Il Regolamento 2024/1689 impiega un approccio basato sul rischio, che si articola in quattro livelli di rischio per i sistemi di IA, e nella identificazione di rischi specifici per i modelli IA per finalità generali:

(1) rischio inesistente: nessun obbligo;

(2) rischio minimo: limitati obblighi, con particolare riferimento alla trasparenza informativa. Ad esempio, laddove esista un evidente rischio di manipolazione (ad esempio, attraverso l'uso di chatbot), gli utenti dovrebbero essere consapevoli del fatto che stanno interagendo con una macchina;

(3) rischio alto: è considerato ad alto rischio un numero limitato di sistemi di IA individuati all'articolo 6 ed elencati nell'Allegato III del Regolamento 2024/1689 che possono potenzialmente avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali. Tali sistemi comprendono anche i componenti di sicurezza dei prodotti disciplinati dalla legislazione settoriale dell'Unione, che saranno sempre considerati ad alto rischio se soggetti a una valutazione della conformità da parte di terzi ai sensi di tale legislazione settoriale;

(4) rischio inaccettabile: una serie molto limitata di usi dell'IA particolarmente dannosi (loe cosiddette "pratiche di intelligenza artificiale") che contravvengono ai valori dell'UE perché violano i diritti fondamentali e saranno pertanto vietati:

1. attribuzione alle persone di un punteggio sociale (*social credit scoring*) per finalità pubbliche e private;
2. sfruttamento delle vulnerabilità delle persone, utilizzo di tecniche subliminali;
3. identificazione biometrica remota in tempo reale in spazi accessibili al pubblico da parte delle autorità pubbliche competenti in materia di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, fatte salve limitate eccezioni in caso di reati gravi;
4. categorizzazione biometrica delle persone fisiche sulla base di dati biometrici per dedurne o desumerne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche o l'orientamento sessuale; sarà ancora possibile filtrare set di dati basandosi su dati biometrici nel settore delle attività di contrasto ai reati;
5. polizia predittiva su singoli;
6. riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione, eccetto per motivi medici o di sicurezza (ad esempio il monitoraggio dei livelli di stanchezza di un pilota);
7. estrazione non mirata di immagini facciali da internet o telecamere a circuito chiuso per la creazione o l'espansione di banche dati (cosiddetto *scraping* on line).

* * * * * * * *

Inoltre, il Regolamento 2024/1689 prende in considerazione i rischi sistemici che potrebbero derivare dai modelli di IA per finalità generali (GPAI) compresi i modelli di IA generativa di grandi dimensioni (LLM models) che possono essere utilizzati per un'ampia serie di compiti e stanno diventando la base di molti sistemi di IA nell'UE. Alcuni di questi modelli potrebbero comportare rischi sistemici se risultano particolarmente efficaci o molto utilizzati. Modelli potenti potrebbero ad esempio causare incidenti gravi o essere utilizzati impropriamente per attacchi informatici di vasta portata.

## Quali criteri sono impiegati dal Regolamento 2024/1689 per classificare un sistema di IA come “ad alto rischio”?

Insieme a una chiara definizione di cosa si intenda per "ad alto rischio", il Regolamento 2024/1689 istituisce una solida metodologia che aiuta a individuare i sistemi di IA ad alto rischio all'interno del quadro giuridico. L'obiettivo è garantire la certezza del diritto per le imprese e gli altri operatori.

Il primo criterio è fissato all’articolo 6 del Regolamento: è ad alto rischio un sistema di IA destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato da direttive settoriali elencate all’Allegato I del Regolamento e soggetto a procedure di valutazione della conformità.

Al Regolamento è poi allegato un elenco di casi d'uso ritenuti ad alto rischio, che la Commissione provvederà a mantenere periodicamente aggiornato agli sviluppi tecnologici.

Ecco gli esempi di casi d'uso di sistemi IA ad alto rischio elencati nell'Allegato III:

- le infrastrutture critiche, ad esempio le infrastrutture digitali o le infrastrutture che utilizzano l’AI nei settori del traffico stradale e della fornitura di acqua, gas, riscaldamento ed elettricità;

- istruzione e formazione professionale, ad esempio i sistemi IA impiegati per valutare i risultati dell'apprendimento e orientare il processo di apprendimento e il monitoraggio dei comportamenti disonesti;

- occupazione, gestione dei lavoratori e accesso al lavoro autonomo, ad esempio i sistemi IA impiegati per pubblicare annunci di lavoro mirati, analizzare e filtrare le candidature e valutare i candidati;

- i sistemi IA impiegati per l’accesso a servizi e a prestazioni pubblici e privati essenziali (ad esempio l'assistenza sanitaria), per la valutazione dell'affidabilità creditizia delle persone fisiche e per la valutazione dei rischi e la determinazione dei prezzi in relazione ad assicurazioni sulla vita e assicurazioni sanitarie;

- alcuni sistemi IA utilizzati nell'ambito delle attività di contrasto, del controllo delle frontiere, dell'amministrazione della giustizia e dei processi democratici;

- i sistemi IA impiegati per la valutazione e classificazione delle chiamate di emergenza;

- sistemi di identificazione biometrica, categorizzazione biometrica e riconoscimento delle emozioni impiegati dalle autorità di contrasto nei casi in deroga al divieto e per i reati più gravi come elencati dal Regolamento 2024/1689.

Non sono ritenuti ad alto rischio – anche se rientranti nell'elenco dell'Allegato III appena sopra fornito - i sistemi IA che svolgono compiti procedurali limitati, migliorano i risultati di precedenti attività umane, non influenzano le decisioni umane o svolgono compiti puramente preparatori.

Non sono inoltre inclusi tra i sistemi IA ad alto rischio i sistemi di raccomandazione delle piattaforme online di dimensioni molto grandi in quanto sono già disciplinati da altre normative, come i due Regolamenti sui servizi digitali (Regolamento 2022/2065) e sui mercati digitali (Regolamento 2022/1925).

Si ricordi infine che un sistema di IA è tuttavia sempre considerato ad alto rischio se esegue la profilazione di persone fisiche.

## Quali sono gli obblighi per i fornitori di sistemi di IA ad alto rischio?

Prima di immettere un sistema di IA ad alto rischio sul mercato dell'UE, o di farlo entrare in servizio, i fornitori devono sottoporlo a una valutazione della conformità**.** Potranno così dimostrare che il loro sistema è conforme ai requisiti obbligatori per un'IA affidabile (ad esempio qualità dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, accuratezza, cibersicurezza e robustezza). Tale valutazione deve essere ripetuta in caso di modifica sostanziale del sistema o della sua finalità.

I sistemi di IA che costituiscono componenti di sicurezza di prodotti disciplinati dalla legislazione settoriale dell'Unione saranno sempre considerati ad alto rischio se soggetti a una valutazione della conformità da parte di terzi ai sensi di tale legislazione settoriale. Anche per i sistemi biometrici è sempre richiesta una valutazione della conformità da parte di terzi.

I fornitori di sistemi di IA ad alto rischio dovranno inoltre attuare sistemi di gestione della qualità e del rischio per garantire la conformità ai nuovi requisiti e ridurre al minimo i rischi per gli utenti e le persone interessate, anche dopo l'immissione sul mercato di un prodotto.

I sistemi di IA ad alto rischio implementati da autorità pubbliche o entità che agiscono per loro conto dovranno essere registrati in una banca dati pubblica dell'UE, a meno che tali sistemi non siano utilizzati per le attività di contrasto e di controllo dell'immigrazione. Questi ultimi sistemi dovranno essere registrati in una parte non pubblica della banca dati, che sarà accessibile solo alle autorità di controllo competenti.

Le autorità di vigilanza del mercato contribuiranno al monitoraggio successivo all'immissione sul mercato mediante audit e offrendo ai fornitori la possibilità di segnalare incidenti o violazioni gravi degli obblighi in materia di diritti fondamentali di cui sono venuti a conoscenza. Qualsiasi autorità di vigilanza del mercato può autorizzare l'immissione sul mercato di una specifica IA ad alto rischio per motivi eccezionali.

In caso di violazione, i requisiti consentiranno alle autorità nazionali di avere accesso alle informazioni necessarie per indagare se l'uso del sistema di IA sia conforme alla legge.

## Gli utilizzatori finali di sistemi di IA ad alto rischio – come, ad esempio, un'azienda che acquista da un fornitore tali sistemi – sono soggetti ad obblighi?

Si. L'articolo 26 del Regolamento 2024/1689 prescrive rilevanti adempimenti – tecnici, organizzativi, documentali e gestionali – in capo al "*deployer*" (ovvero: "*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*").

Gli utilizzatori finali devono infatti:

(1) adottare idonee misure tecniche e organizzative per garantire di utilizzare i sistemi IA ad alto rischio conformemente alle istruzioni per l'uso che accompagnano i sistemi;
(2) affidare la sorveglianza umana sulla operatività dei sistemi IA ad alto rischio a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario;
(3) conservare i *logs* generati automaticamente dal sistema di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo, per almeno sei mesi;
(4) informare i rappresentanti dei lavoratori – secondo le relative procedure sindacali - e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio, e ciò prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro;
(5) nella misura in cui esercitano il controllo sui dati di input, garantire che tali dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista del sistema di IA ad alto rischio;
(6) monitorare l'operatività dei sistemi IA ad alto rischio, prevedendo procedure tecniche di sospensione o interruzione in caso di indicenti;
(7) notificare gli incidenti gravi al fornitore, al distributore e alle autorità di vigilanza del mercato;
(8) effettuare la valutazione di impatto dui dati personali ai sensi dell'articolo 35 del Regolamento 679/2016 (avvalendosi anche delle specifiche informazioni sul sistema IA ad alto rischio di cui all'articolo 13 del Regolamento 2024/1689);
(9) informare gli interessati se vengono impiegati sistemi di IA ad alto rischio di cui all'allegato III che adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche;
(10) svolgere la valutazione di impatto sui diritti e le libertà fondamentali di cui all'articolo 27 del Regolamento 2024/1689, ma solamente nel caso in cui l'utilizzatore sia un soggetto pubblico oppure un privato che utilizza sistemi di IA per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito (ad eccezione dei sistemi di IA utilizzati allo scopo di individuare frodi finanziarie) oppure per valutare i rischi e determinare i prezzi in relazione a persone fisiche nel caso di assicurazioni sulla vita e assicurazioni sanitarie.

## Come sono disciplinati i modelli di IA per finalità generali?

I modelli di IA per finalità generali, compresi i modelli di IA generativa di grandi dimensioni (es: CHAT-GPT), possono essere utilizzati per vari compiti. I singoli modelli possono essere integrati in un gran numero di sistemi di IA. È importante che un fornitore che intenda basarsi su un

modello di IA per finalità generali disponga di tutte le informazioni necessarie per fare in modo che il suo sistema sia sicuro e conforme alla legge sull'IA.

Il Regolamento 2024/1689 obbliga di conseguenza i fornitori di tali modelli a comunicare determinate informazioni ai fornitori di sistemi a valle. Una siffatta trasparenza rende possibile una migliore comprensione di tali modelli.

È altresì necessario che i fornitori di modelli dispongano di politiche in essere atte a garantire il rispetto del diritto d'autore nel corso della formazione dei loro modelli.

Alcuni di questi modelli potrebbero inoltre comportare rischi sistemici dato che sono particolarmente efficaci o molto utilizzati.

Per il momento il Legislatore UE ritiene che i modelli di IA per finalità generali che sono stati addestrati utilizzando una potenza di calcolo totale superiore a 10^25 FLOPS comportino rischi sistemici, dato che i modelli addestrati con una potenza di calcolo più elevata tendono ad essere più potenti. L'Ufficio per l'IA (istituito all'interno della Commissione e già operativo) può aggiornare tale soglia alla luce dell'evoluzione tecnologica e può inoltre, in casi specifici, designare altri modelli in quanto tali sulla base di ulteriori criteri (ad esempio il numero di utenti o il grado di autonomia del modello).

I fornitori di modelli che comportano rischi sistemici sono pertanto tenuti a valutare e attenuare i rischi, a segnalare incidenti gravi, a condurre prove e valutazioni dei modelli all'avanguardia, a garantire la cibersicurezza e a fornire informazioni sul consumo energetico dei loro modelli.

A tal fine sono invitati a collaborare con l'Ufficio europeo per l'IA per elaborare codici di condotta che siano uno strumento centrale per precisare le norme in cooperazione con altri esperti. Un gruppo di esperti scientifici svolgerà un ruolo centrale nella supervisione dei modelli di IA per finalità generali.

## Come è disciplinata l'identificazione biometrica nel Regolamento 2024/1689?

L'uso dell'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico (ossia il riconoscimento facciale mediante telecamere a circuito chiuso) a fini di contrasto è vietato, a meno che non sia utilizzato in uno dei seguenti casi:

- attività di contrasto relative a 16 reati specifici;
- ricerca mirata di specifiche vittime, rapimento, tratta e sfruttamento sessuale di esseri umani e persone scomparse;
- prevenzione di minacce per la vita o l'incolumità fisica delle persone o risposta a una minaccia attuale o prevedibile di attacco terroristico.

L'elenco dei 16 reati contiene:

- terrorismo;

- tratta di esseri umani;
- sfruttamento sessuale di minori e materiale pedopornografico,
- traffico illecito di stupefacenti e sostanze psicotrope,
- traffico illecito di armi, munizioni ed esplosivi,
- omicidio volontario;
- lesioni personali gravi;
- traffico illecito di organi e tessuti umani;
- traffico illecito di materie nucleari e radioattive,
- rapimento, sequestro e presa di ostaggi;
- reati che rientrano nella competenza giurisdizionale della Corte penale internazionale,
- dirottamento di un aeromobile/una nave;
- stupro;
- reati ambientali:
- furto organizzato o rapina a mano armata;
- sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra.

L'identificazione biometrica remota in tempo reale da parte delle autorità di contrasto è subordinata a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o amministrativa indipendente, la cui decisione è vincolante. In caso di urgenza l'autorizzazione può essere rilasciata entro 24 ore; se l'autorizzazione non è concessa, è necessario che tutti i dati e gli output siano soppressi.

L'autorizzazione deve essere preceduta da una valutazione preventiva d'impatto sui diritti fondamentali e deve essere notificata all'autorità di vigilanza del mercato e all'autorità per la protezione dei dati interessate. In situazioni di urgenza, è possibile iniziare a usare il sistema senza registrazione.

L'uso di sistemi di IA per l'identificazione biometrica remota a posteriori (identificazione di persone in materiale video raccolto in precedenza) delle persone oggetto di indagine richiede l'autorizzazione preventiva di un'autorità giudiziaria o di un'autorità amministrativa indipendente e la notifica all'autorità per la protezione dei dati e all'autorità di vigilanza del mercato.

**Cos'è una valutazione d'impatto sui diritti fondamentali? Chi deve effettuare tale valutazione? Quando deve essere effettuata?**

L'uso di un sistema di IA ad alto rischio può avere un impatto sui diritti fondamentali. Pertanto:

1. gli organismi di diritto pubblico;
2. i privati che forniscono servizi pubblici;
3. i privati che utilizzano sistemi di IA ad alto rischio per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito (ad eccezione dei sistemi di IA utilizzati allo scopo di individuare frodi finanziarie) oppure per valutare i rischi e determinare i prezzi in relazione a persone fisiche nel caso di assicurazioni sulla vita e assicurazioni sanitarie;

devono effettuare una valutazione dell'impatto sui diritti fondamentali e comunicarne i risultati all'autorità nazionale (in Italia al momento si è scelto di assegnare il ruolo di autorità nazionale per l'IA all'AgID e all'Autorità Nazionale per la Cybersicurezza – ACN).

La valutazione consiste in una descrizione dei processi dell'operatore in cui il sistema di IA ad alto rischio sarà utilizzato, del periodo di tempo e della frequenza in cui il sistema di IA ad alto rischio è destinato a essere utilizzato, delle categorie di persone fisiche e dei gruppi che possono essere interessati dal suo uso nel contesto specifico, dei rischi specifici di danno che possono incidere sulle categorie di persone o sui gruppi di persone interessati, e in una descrizione dell'attuazione delle misure di sorveglianza umana e delle misure da adottare in caso di concretizzazione dei rischi.

Se il soggetto tenuto ha già soddisfatto l'obbligo attraverso la valutazione d'impatto sulla protezione dei dati personali richiesta dall'articolo 35 del Regolamento 679/2016 - GDPR la valutazione d'impatto sui diritti fondamentali deve essere effettuata congiuntamente a tale valutazione d'impatto sulla protezione dei dati.

## Quale sistema di governance a livello europeo e nazionale è introdotto dal Regolamento 2024/1689?

Gli Stati membri svolgono un ruolo chiave nell'applicare il regolamento e nel garantirne il rispetto. A tal proposito ciascuno Stato membro deve designare una o più autorità nazionali competenti incaricate di supervisionarne l'applicazione e l'attuazione, nonché di svolgere attività di vigilanza del mercato.

Per aumentare l'efficienza e istituire un punto di contatto ufficiale con il pubblico e le altre controparti, ciascuno Stato membro deve designare un'autorità nazionale di controllo, che rappresenterà anche il paese nell'ambito del Comitato europeo per l'intelligenza artificiale.

Ulteriori competenze tecniche saranno fornite da un forum consultivo in cui è rappresentata una selezione equilibrata di portatori di interessi, tra cui l'industria, le start-up, le PMI, la società civile e il mondo accademico.

La Commissione ha inoltre già istituito e fatto entrare in servizio il nuovo Ufficio europeo per l'IA, nell'ambito della Commissione, che supervisiona i modelli di IA per finalità generali, coopera con il Comitato europeo per l'intelligenza artificiale e sarà sostenuto da un gruppo di esperti scientifici indipendenti.

## Quali sono le sanzioni in caso di violazione del Regolamento 2024/1689?

Per i sistemi di IA che sono immessi sul mercato o messi in servizio e che non rispettano i requisiti del Regolamento 2024/1689, gli Stati membri dovranno stabilire sanzioni effettive, proporzionate e dissuasive, comprese sanzioni amministrative pecuniarie, in relazione alle violazioni e comunicarle alla Commissione.

Il Regolamento stabilisce le soglie da tenere in considerazione:

- fino a 35 milioni di € o al 7 % del fatturato mondiale totale annuo dell'esercizio precedente (se superiore) per violazioni relative a pratiche vietate o per l'inosservanza di requisiti in materia di dati;
- fino a 15 milioni di € o al 3 % del fatturato mondiale totale annuo dell'esercizio precedente per l'inosservanza di qualsiasi altro requisito o obbligo del Regolamento, compresa la violazione delle regole relative ai modelli di IA per finalità generali;
- fino a 7,5 milioni di € o all'1,5 % del fatturato mondiale totale annuo dell'esercizio precedente per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti in risposta a una richiesta;
- per ciascuna categoria di violazione, la soglia per le PMI sarà l'importo più basso tra i due previsti, mentre per le altre imprese sarà l'importo più elevato.

La Commissione, sulla base del parere del comitato, elaborerà orientamenti al fine di armonizzare le regole e le prassi nazionali in materia di calcolo delle sanzioni amministrative pecuniarie.

Poiché dovrebbero dare l'esempio, le istituzioni, le agenzie o gli organismi dell'UE non beneficeranno di deroghe: il Garante europeo della protezione dei dati avrà il potere di infliggere loro sanzioni pecuniarie.

## Cosa sono le sandbox regolatorie nel settore dell'Intelligenza Artificiale?

Il Regolamento 2024/1689 introduce la disciplina delle cosiddette sandbox sull'IA, anche note come spazi di sperimentazione normativa e di prova in condizioni reali di mercato, che forniscono un ambiente controllato per testare tecnologie innovative per un periodo di tempo limitato, promuovendo in tal modo l'innovazione da parte delle imprese, delle PMI e delle start-up. Gli spazi di sperimentazione normativa, insieme ad altre misure quali le reti dei centri di eccellenza per l'IA, il partenariato pubblico-privato sull'intelligenza artificiale, i dati e la robotica e l'accesso ai poli dell'innovazione digitale e alle strutture di prova e sperimentazione, contribuiranno a creare le giuste condizioni quadro affinché le imprese sviluppino e implementino l'IA.

Le prove in condizioni reali dei sistemi di IA ad alto rischio possono essere effettuate per un massimo di 6 mesi (prorogabili di altri 6 mesi). Prima delle prove deve essere elaborato un piano che deve essere presentato all'autorità di vigilanza del mercato, la quale deve approvare il piano e le condizioni di prova specifiche; in caso di mancata risposta entro 30 giorni, il piano si considera automaticamente approvato in modo tacito. Le prove possono essere oggetto di ispezioni senza preavviso da parte dell'autorità.

Le prove in condizioni reali possono essere effettuate solo se sono presenti garanzie specifiche, ad esempio gli utenti dei sistemi sottoposti a prova in condizioni reali devono fornire un consenso informato, le prove non devono avere alcun effetto negativo sugli utenti, gli esiti delle

prove devono essere reversibili o devono poter essere ignorati, e i loro dati devono essere cancellati dopo la conclusione delle prove. Una protezione speciale deve essere concessa ai gruppi vulnerabili, ad esempio a causa della loro età o della disabilità fisica o mentale.