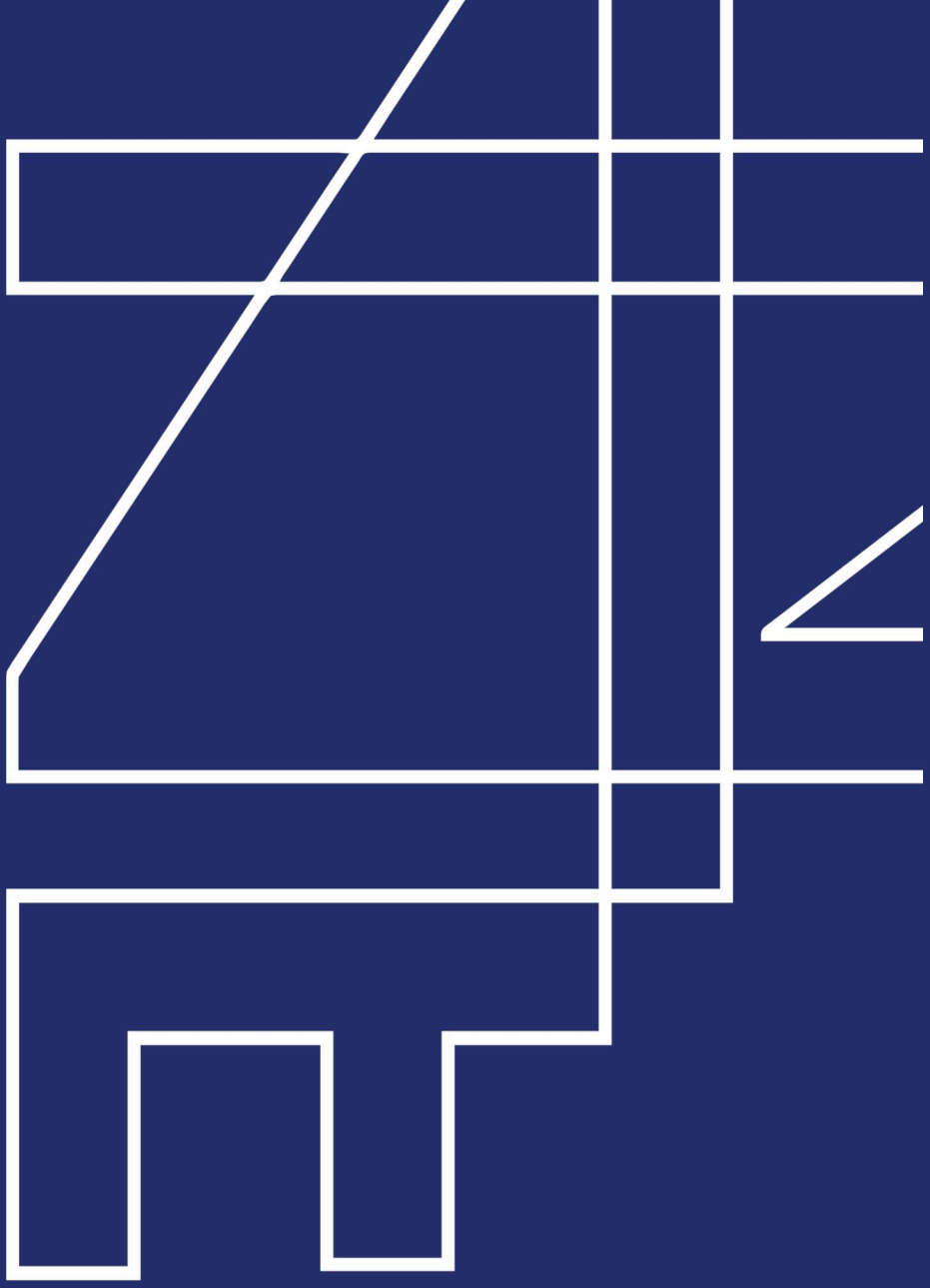

Policy Paper

Il Regolamento UE 2024 /1689. - AI ACT

I contenuti e i nuovi obblighi per le imprese

Febbraio 2025

Anitec-Assinform

Anitec-Assinform

Realizzato da:

Anitec-Assinform e Qubit Law Firm & Partners

Revisione editoriale a cura di:

Anitec-Assinform e Qubit Law Firm & Partners

Anitec-Assinform

Sommario

SINTESI DEI CONTENUTI – PUNTI CHIAVE

Obiettivi e contesto dell'AI Act

Scopo principale: promuovere lo sviluppo e l'adozione di un'intelligenza artificiale antropocentrica, affidabile e conforme ai valori europei, garantendo un livello elevato di protezione della salute, sicurezza e diritti fondamentali.

Strategia europea: l'AI Act è inserito in una cornice più ampia di politiche europee che mirano a sostenere l'innovazione, ridurre gli oneri normativi per le PMI e promuovere la fiducia nell'IA attraverso un approccio basato sul rischio.

Struttura del regolamento

Divieti assoluti: sistemi IA con rischi inaccettabili, ad esempio per manipolazione, sfruttamento di vulnerabilità o riconoscimento biometrico in tempo reale in spazi pubblici, salvo eccezioni molto limitate.

Pratica di IA vietata	Esempio
Tecniche subliminali e sfruttamento di vulnerabilità	Ipotetico servizio di streaming che inserisce messaggi subliminali nei video o nei film, o chatbot "sentimentali" che inducono manipolatoriamente azioni dannose per la salute o gli interessi finanziari dell'utente.
Social scoring	Il sistema utilizzato in Cina che assegna punteggi sociali ai cittadini in base al loro comportamento, limitando l'accesso a servizi come la richiesta del passaporto o la frequenza di certi istituti scolastici.
Giustizia predittiva	Il software COMPAS negli USA che valutava la probabilità di recidiva basandosi su fattori esterni come amicizie e quartiere di residenza, risultando discriminatorio verso le persone di colore.
Creazione di banche dati per riconoscimento facciale	Il caso Clearview, sanzionato dal Garante italiano, che aveva creato una banca dati attraverso lo *scraping* di immagini dai social network e dalle telecamere a circuito chiuso.
Inferenza di emozioni (vietato in ambiente educativo e sul lavoro con eccezioni per motivi sanitari e di sicurezza)	Sistema di IA che analizza le espressioni del viso degli studenti durante gli esami.
Classificazioni biometriche	Il sistema cinese IJOP (Integrated Joint Operation Platform) che identifica e traccia gli Uiguri basandosi sulle caratteristiche somatiche
Identificazione biometrica in tempo reale (con eccezioni relative a casi specifici)	Utilizzo di sistemi di riconoscimento facciale in spazi pubblici (da parte di forze dell'ordine) per riconoscere le persone dai filmati delle telecamere, in tempo reale

Tabella 1. Pratiche di IA viatetate, esempi.

Sistemi ad alto rischio: per casi d'uso in settori specifici (es. sanità, lavoro, credito) vengono introdotti requisiti di conformità dei sistemi, inclusa la documentazione tecnica e il monitoraggio.

Sistema ad alto rischio (prodotti o componenti di sicurezza di prodotti), normativa di riferimento	**Esempio**
Direttiva 2006/42/CE **che disciplina la sicurezza delle macchine e dei loro componenti.**	Sistema IA che controlla i sensori di sicurezza di un robot industriale per evitare collisioni con gli operatori
Direttiva sulla sicurezza dei **giocattoli** (2009/48/CE)	IA che gestisce i sistemi di limitazione della velocità in un giocattolo elettrico cavalcabile per bambini
Direttiva 2013/53/UE sulle **imbarcazioni da diporto e normativa IMO**	Sistema IA che gestisce il controllo automatico della navigazione e prevenzione delle collisioni
Direttiva 2014/33/UE sugli **ascensori e i componenti di sicurezza**	IA che monitora e controlla i sistemi di frenata di emergenza degli ascensori
Direttiva 2014/34/UE (ATEX), che **regolamenta l'attrezzatura destinata ad atmosfere esplosive.**	Sistema IA che monitora e regola i sensori di gas in ambienti ATEX
Direttiva 2014/53/UE sulla compatibilità elettromagnetica e le **apparecchiature radio**	IA che gestisce i sistemi di protezione dalle interferenze in apparecchiature radio critiche
Direttiva 2014/68/UE sulle **attrezzature a pressione**	Sistema IA che controlla le valvole di sicurezza in caldaie industriali
Regolamento (UE) 2016/424 **sugli impianti a fune (funivie e impianti simili)**	IA che gestisce i sistemi di frenata emergenza nelle funivie
Regolamento (UE) 2016/425 sui **dispositivi di protezione individuale**	Sistema IA integrato in un respiratore che regola il flusso d'aria in base alle condizioni ambientali
Regolamento (UE) 2016/426 **sugli apparecchi a gas**	IA che controlla i sistemi di spegnimento automatico in caso di perdite di gas
Regolamento (UE) 2017/745 **sui dispositivi medici**	Sistema IA che controlla i parametri vitali in un ventilatore polmonare

Regolamento (UE) 2017/746 sui **dispositivi diagnostici in vitro**	IA che analizza immagini mediche per rilevare patologie critiche
Regolamento (CE) 300/2008 che istituisce norme comuni per la **sicurezza dell'aviazione civile**	Sistema IA per il controllo automatico del traffico aereo
Regolamento (UE) 168/2013 sui **veicoli a due/tre ruote e quadricicli**	IA che gestisce i sistemi anti-bloccaggio freni in veicoli
Regolamento (UE) 167/2013 **sui veicoli agricoli e forestali**	Sistema IA che controlla i sistemi di sicurezza anti-ribaltamento nei trattori
Direttiva 2014/90/UE **sull' equipaggiamento marittimo**	IA che gestisce i sistemi di navigazione automatica nelle navi
Direttiva (UE) 2016/797 relativa **all'interoperabilità del sistema ferroviario**	Sistema IA che controlla i sistemi di segnalamento e frenata dei treni
Regolamento (UE) 2018/858 che stabilisce le norme **per l'omologazione e la vigilanza del mercato dei veicoli a motore, dei loro rimorchi, e dei sistemi, componenti e unità tecniche indipendenti destinati a tali veicoli.**	IA che gestisce i sistemi di frenata automatica di emergenza nelle auto
Regolamento (UE) 2018/1139, recante norme comuni **nel settore dell'aviazione civile.**	Sistema IA che controlla il rilevamento e l'evitamento di ostacoli nei droni

Tabella 2. Sistemi ad alto rischio che sono prodotti o componenti di sicurezza di prodotti, normativa di riferimento e Esempi

Sistema ad alto rischio Stand Alone	Esempi
Identificazione/Categorizzazione Biometrica	Sistema di riconoscimento facciale in aeroporti, Sistema di analisi delle emozioni durante colloqui di lavoro
Gestione Infrastrutture Critiche	IA per gestione rete elettrica nazionale, Sistema di controllo del traffico autostradale, IA per gestione rete idrica urbana
Istruzione e Formazione	Sistema di valutazione automatica per ammissione università, IA per monitoraggio esami online, Software per valutazione automatica dei test
Occupazione e Lavoro	ATS (Applicant Tracking System) per screening CV, IA per valutazione performance dipendenti, Sistema per assegnazione turni basato su comportamenti
Accesso Servizi Essenziali	IA per valutazione eligibilità sussidi sociali, Sistema di credit scoring bancario, IA per triage ospedaliero, Software per calcolo premi assicurativi
Attività di Contrasto	Sistema predittivo per rischio vittimizzazione, IA per analisi affidabilità prove in tribunale, Software per valutazione rischio recidiva
Migrazione e Frontiere	Sistema per screening visti, IA per analisi rischio sicurezza ai confini, Software per esame domande asilo
Giustizia e Processi Democratici	IA per ricerca precedenti legali e interpretazione normativa, Sistema per analisi comportamento elettorale (esclusa logistica campagne)

Tabella 3. Esempi di sistemi ad alto rischio "Stand Alone"

Sistemi a rischio limitato: obblighi di trasparenza, come nel caso di chatbot che devono dichiarare la loro natura non umana.

Soggetti coinvolti

Fornitori: responsabili dello sviluppo e della messa sul mercato dei sistemi IA, indipendentemente dalla loro ubicazione geografica.

Deployer: soggetti che utilizzano i sistemi IA nell'UE, con obblighi di monitoraggio e conformità.

Importatori e distributori: devono garantire la conformità dei sistemi IA che introducono nel mercato europeo.

Obblighi normativi

Per i fornitori di sistemi ad alto rischio: garanzia di tracciabilità, certificazione, registrazione in database europei e conformità agli standard di sicurezza.

Per gli utilizzatori: monitoraggio costante delle performance e segnalazione di eventuali anomalie o malfunzionamenti.

Sistemi di IA ad alto rischio	
Requisiti del sistema	**Obblighi del fornitore**
Sistema di gestione dei rischi lungo l'intero ciclo di vita del sistema di IA.	Documentazione del sistema di gestione di qualità
Qualità dei dataset di addestramento	Apposizione dei riferimenti identificativi del fornitore (sul sistema o sulla documentazione)
Documentazione tecnica per dimostrare conformità	Conservazione per 10 anni della documentazione di conformità
Registrazione delle operazioni (logging)	Sottoporre il sistema a valutazione di conformità (interna / esterna) e redigere la dichiarazione di confomità
Trasparenza by design	Etichettatura CE
Misure di supervisione umana	Registrarsi e registrare i sistemi di IA ad alto rischio forniti nella banca dati UE
Accuratezza, robustezza e cybersecurity	Monitoraggio del sistema post-immissione e adozione misure correttive
	Rispettare requisiti di accessibilità
	Nomina rappresentante autorizzato in UE (se nececessario)

Tabella 4. Requisiti del sistema e obblighi dei forntiori per sistemi di IA ad alto rischio.

Obblighi per i fornitori di Modelli GPAI	
Modelli GPAI	**Modelli GPAI a rischio sistemico (in aggiunta a quelli generali)**
Watermarking dei contenuti generati	Effettuare valutazione di conformità al fine di identificare e mitigare il rischio
Redazione documentazione tecnica con informazioni di cui Allegato XI	Valutare e mitigare i rischi sistemici
Messa a disposizione dei fornitori a valle della documentazione con almeno le informazioni di cui all'Allegato XIII	Tenere traccia e comunicare a Ufficio IA e Autorità nazionali i gravi incidenti
Policy per il rispetto del diritto d'autore	Adottare misure correttive per affrontare gravi incidenti
Pubblicare sintesi dettagliata dei dati di addestramento (template da Ufficio IA)	Cybersecurity (informatica e fisica) del modello
Nomina rappresentante UE	Adesione Codici di condotta (facoltativo)
Adesione a Codice di buone pratiche (facoltativo)	

Tabella 5. Obblighi per i fornitori di Modelli GPAI, a rischio sistemico e non.

Governance ed enforcement

Struttura a due livelli: autorità nazionali ed europee coordinate per garantire l'applicazione uniforme delle norme.

Sanzioni: introduzione di sanzioni pecuniarie e di provvedimenti che possono comprendere il ritiro dal mercato dei sistemi non conformi.

Indicazioni di per le imprese

Investire in competenze specifiche e governance dei dati.

Prepararsi alla compliance con il nuovo regolamento attraverso un'adeguata organizzazione interna.

Valutare il ruolo strategico nella catena del valore dell'IA, inclusa la gestione delle relazioni con i partner.

1. Il Regolamento UE 2024/1689: scopo e oggetto della regolamentazione

L'AI Act (di seguito anche "Regolamento") definisce il "sistema di intelligenza artificiale" (art. 3 n. 1, Cons. 12).

"Un sistema di IA è caratterizzato da capacità inferenziali che consentono di generare risultati (output) influenzando l'ambiente fisico o virtuale in cui operano. I sistemi di IA sono progettati per funzionare con livelli di autonomia variabile e possono adattarsi dinamicamente al contesto d'uso."

Per cui, il sistema di IA deve essere:

- progettato per funzionare con livelli di autonomia variabile rispetto all'intervento/coinvolgimento umano;
- variamente adattabile dopo la diffusione/messa in funzione, ossia capace di adeguarsi al contesto dinamico in cui si inserisce;
- caratterizzato da capacità inferenziale, ossia di generare, a partire dagli input che riceve, per obiettivi impliciti o espliciti, output quali contenuti, previsioni, raccomandazioni o decisioni.

È un'impostazione che proviene dalla natura di normativa di prodotto dell'AI Act e che discende, appunto, dall'aver classificato i sistemi di IA come prodotti.

I sistemi di Intelligenza Artificiale (IA) possono essere, infatti, distribuiti in vari modi, come il ***download*** da parte dell'utente sul proprio dispositivo o infrastruttura IT, la fornitura tramite un supporto fisico o l'accesso attraverso un'interfaccia *on line*. Dal punto di vista normativo, queste diverse modalità di impiego possono essere ricondotte a un sistema di IA fornito come prodotto o come servizio.

Durante la fase di stesura dell'AI Act è stata effettuata una scelta, basata su un principio di equivalenza funzionale, non differenziando le regole a seconda che il sistema di IA fosse utilizzato come prodotto o come servizio, ma trattando qualsiasi sistema come un prodotto.

Il Regolamento, quindi, adotta lo schema normativo del Nuovo Quadro Legislativo (NLF) relativo alla sicurezza dei prodotti, considerando il "fornitore" del sistema IA come il "fabbricante" della tradizionale legislazione europea sui prodotti.

Da tali considerazioni emerge anche l'ampio ambito di applicazione dell'AI Act, chiarito nel Considerando 12, dato che i sistemi di IA possono essere utilizzati come elementi indipendenti (stand-alone) oppure essere componenti di un prodotto o di un sistema più ampio, al quale possono essere incorporati oppure no (art. 2 e art. 6 par. 1 e 2).

Stante il requisito contenuto nella definizione secondo cui un sistema IA ha capacità inferenziali, sono esclusi dall'applicazione delle norme dell'AI Act tutti quei software tradizionali che operano con programmazione deterministica.

Il Regolamento **non si applica** (art. 2):

- ai sistemi di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici, ed alle attività di ricerca, prova o sviluppo anteriori all'immissione sul mercato (par. 2, Cons. 25);
- i sistemi di IA immessi sul mercato, messi in servizio o utilizzati esclusivamente per scopi militari, di difesa o sicurezza nazionale (par. 2, Cons. 24);
- l'utilizzo di sistemi di IA da parte di autorità pubbliche di Paesi terzi o organizzazioni internazionali nel quadro della cooperazione o di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'UE o con gli Stati membri, sempre che il Paese terzo o l'organizzazione internazionale fornisca garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali (par. 2, cons. 27);
- ai sistemi di IA rilasciati con licenza libera o open source, tranne che rientrino nella categoria di alto rischio o tra quelli vietati (art. 5) o destinati ad interagire con le persone (art. 50);
- ai deployer che utilizzano sistemi di IA nel corso di un'attività non professionale puramente personale.

L'impianto originario dell'AI Act come norma di prodotto è stato in parte alterato con l'introduzione di norme specifiche per i modelli di IA per finalità generali (General Purpose AI - GPAI), i c.d. modelli fondazionali (art. 3, n. 63 e Cons. 97).

La disciplina dei modelli di IA per finalità generali ha fatto compiere un salto "upstream" all'AI Act, andando a disciplinare componenti che possono porsi a monte di un sistema di IA.

Nello specifico, sono definiti come modelli di IA per finalità generali quelli:

- caratterizzati da generalità significativa;
- capaci di svolgere con competenza un'ampia gamma di compiti;
- idonei a essere integrati in sistemi o applicazioni diverse;

ciò indipendentemente dal fatto che il modello sia stato addestrato con grandi quantità di dati utilizzando tecniche di *machine learning*.

Gli obblighi sono collegati alla semplice immissione sul mercato del modello, indipendentemente dalle modalità con cui essa avviene (ad esempio tramite librerie software o API) e non si applicano a modelli utilizzati solo per ricerca, sviluppo o prototipazione prima di essere immessi sul mercato.

A sua volta un **sistema di IA per finalità generali** sarà il sistema che utilizza un modello di IA per finalità generali e che può perseguire varie finalità, sia per uso diretto sia per integrazione in altri sistemi di IA (art. 3, n. 66).

2. Applicazione e soggetti dell'AI Act: come identificare all'interno della catena di fornitura, per ciascun sistema di IA, il fornitore, il deployer e le altre figure

2.1. Qualifica di fornitore (art. 3, n 3):

Il fornitore è definito come la persona fisica o giuridica che sviluppa un sistema di IA o lo fa sviluppare sotto la propria direzione e controllo e immette il sistema sul mercato dell'UE o lo mette in servizio (anche per uso proprio).

Può essere un'azienda con sede nell'UE o in un paese terzo, a condizione che il sistema sia immesso o messo in servizio nel mercato dell'Unione.

I fornitori devono garantire sia la conformità normativa, sia gestire il governo dei dati e i rischi associati al sistema IA.

2.2. Qualifica di deployer (art. 3, n. 4):

Il deployer è la persona fisica o giuridica che utilizza un sistema di IA nell'ambito della propria attività professionale, sotto la propria autorità e controllo. Ad esempio: un'azienda che usa un chatbot basato su IA per il servizio clienti non è il fornitore della chatbot, ma il deployer.

I deployer sono soggetti agli obblighi del regolamento se operano nell'UE ed utilizzano l'output del sistema IA all'interno dell'Unione, anche se sviluppato in un paese terzo.

2.3. Altri operatori nella catena del valore

Importatori: chi immette sul mercato dell'UE un sistema di IA sviluppato da soggetti situati in paesi terzi (art. 3, n.6).

Distributori: chi rende disponibile sul mercato un sistema di IA senza essere fornitore o importatore (art. 3, n. 7).

Fabbricanti di prodotti integrati con IA: se il sistema IA è parte di un prodotto, il fabbricante assume anche gli obblighi del fornitore (art. 22).

Rappresentanti autorizzati: i fornitori non stabiliti nell'UE devono nominare un rappresentante per i sistemi IA ad alto rischio (artt. 25, 54).

L'applicazione del Regolamento dipende dall'utilizzo del sistema IA o dell'utilizzo del suo output nell'UE: è stato, infatti, adottato tale approccio per evitare elusioni normative, ad esempio nei casi di esternalizzazione fuori dall'UE.

In altri termini, l'AI Act intende garantire un level playing field tra operatori UE ed extra-UE, salvaguardando i diritti fondamentali.

Perciò il Regolamento assegna obblighi specifici e diversificati a fornitori, deployer e altri soggetti della supply chain, al fine di assicurare un utilizzo sicuro e responsabile dell'IA nell'UE

Ciò comporta che ogni operatore deve identificare il proprio ruolo nella catena del valore per adempiere correttamente agli obblighi previsti dal Regolamento.

2.4. Criteri di applicazione della normativa

L'art. 2 dell'AI Act prevede la sua applicazione ai fornitori (produttori) che immettono sul mercato o mettono in servizio sistemi di IA o modelli di IA per finalità generali nell'Unione Europea, e ciò indipendente se essi siano stabiliti o situati nell'Unione o in un paese terzo.

Unitamente alla classica fattispecie della disciplina dei prodotti circa l'immissione sul mercato è stata inserita l'ulteriore ipotesi di "**messa in servizio" nell'Unione**, evidentemente alla luce del fatto che un sistema IA composto dal solo *software* può essere erogato, come servizio, da qualsiasi apparecchiatura *hardware* collocata al di fuori della UE.

La previsione include non solo la messa a disposizione del sistema, ma anche la possibilità data a soggetti che si trovano nel mercato europeo di accedere a modelli di IA per uso generale, indipendentemente dal territorio in cui tale modello viene messo a disposizione. La norma è volta, evidentemente, a regolare i fenomeni di messa a disposizione degli utenti non solo tramite interfacce apposite (*chatbot* o altri sistemi) ma anche mediante *Application Programming Interface* (API).

Il Regolamento n. 2024/1689 trova applicazione anche nei confronti dei *deployer* che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione. Il termine *deployer,* che anche nella versione italiana è riportato in

lingua inglese, è definito come "*una persona fisica o giuridica, 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*". Si tratta, quindi, di un soggetto che **nella propria attività professionale** utilizza un sistema di IA. La locuzione "sotto la propria autorità" è in verità ambigua, ed il Considerando n. 13 non fornisce chiarimenti in tal senso.

Si tratta comunque di un soggetto che entra nella "AI *value chain*" come colui che pone in uso il sistema AI (per usi professionali), e comprende sia i casi di sviluppo esterno sia interno (ad es. un'azienda che decida di utilizzare un sistema di IA nell'ambito della gestione dei lavoratori).

Gli altri soggetti inclusi nella AI *value chain* sono gli importatori e distributori di sistemi di IA, i fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e i rappresentanti autorizzati di fornitori non stabiliti nell'Unione.

L'AI Act si applica anche a fornitori e *deployer* di sistemi che sono situati in un paese terzo, quando l'output prodotto dal sistema AI è utilizzato nell'Unione Europea. L'ipotesi intende coprire i casi in cui un soggetto stipuli, ad esempio, un contratto di fornitura con un soggetto terzo collocato extra-UE che per erogare il servizio utilizzi un sistema di IA, anche eventualmente proibito o ad alto rischio, e l'output prodotto venga poi utilizzato all'interno dell'Unione.

La previsione stabilisce che l'output (contenuto, previsioni, raccomandazioni e decisioni) sia effettivamente utilizzato all'interno della UE, non solamente in via ipotetica. In tale ipotesi è sufficiente che il risultato delle elaborazioni svolte da un sistema IA venga utilizzato in Unione Europea affinché tali soggetti rientrino nell'alveo applicativo della disciplina.

L'art. 2, par. 1, lett. g) prevede la propria applicabilità alle "*persone interessate che si trovano nell'Unione*". La locuzione è talmente ampia da comprendere tutti i soggetti che utilizzano un sistema di IA all'interno dell'Unione, ed è volta principalmente, in considerazione della struttura dei vari requisiti e adempimenti stabiliti nel testo regolamentare, all'applicazione delle previsioni in tema di pratiche di IA vietare, trasparenza e disciplina dei modelli di IA con finalità generali da parte degli utilizzatori degli stessi.

In sintesi, i criteri di collegamento territoriale che rendono applicabile la disciplina dell'AI Act sono:

- l'immissione o messa in servizio nel mercato europeo per i fornitori;
- l'utilizzo per scopi professionali da parte di soggetti stabiliti o situati in UE;
- l'utilizzo degli output in Unione Europea, per fornitori o deployer che sono stabiliti extra-UE;
- importatori e distributori di sistemi IA in UE;
- l'immissione di un prodotto a cui è associato un sistema di IA con nome o marchio del fabbricante del prodotto.

Sono quindi esclusi dall'applicazione dell'AI Act i prodotti o sistemi di IA che sono sviluppati in UE, ma messi in commercio o in servizio unicamente al di fuori dell'Unione Europea.

3. La classificazione e gli obblighi per i sistemi di IA

L'AI Act prevede dei divieti assoluti per alcune "pratiche di IA" il cui rischio è considerato inaccettabile, requisiti obbligatori per i sistemi di IA ad alto rischio. Sono inoltre stabiliti obblighi di trasparenza per i sistemi che interagiscono direttamente con le persone fisiche, nonché specifiche disposizioni volte a favorire il consapevole utilizzo, anche da parte di chi vuole integrarli in propri sistemi di IA, dei modelli di IA per finalità generali (con prescrizioni rafforzate per quelle che presentano dei rischi sistemici) fino a includere la promozione di codici di condotta e buone pratiche per il raggiungimento degli obiettivi del regolamento (art. 26 e 27).

La classificazione dei sistemi di IA è rapportata al livello di rischio che comporta il loro utilizzo per la salute, la sicurezza e i diritti fondamentali delle persone prevedendo, per l'appunto, le seguenti categorie principali:

- **Rischio inaccettabile**: pratiche vietate (art. 5).
- **Alto rischio**: sistemi soggetti a requisiti di conformità e obblighi per i produttori (art. 6-49).

- **Modelli fondazionali con rischio sistemico**: si tratta dei modelli di IA per finalità generali che per loro capacità possono determinare un rischio sistemico in Unione Europea (art. 51 ss.)
- **Rischio limitato**: sistemi con obblighi di trasparenza per prevenire inganni o manipolazioni (art. 50) compreso l'utilizzo di modelli di IA per finalità generali.
- **Rischio minimo o assente**: sistemi non soggetti a obblighi specifici, ma viene incoraggiata l'adozione di codici di condotta.

La classificazione è visualizzabile come una piramide, con il rischio inaccettabile al vertice (Fig. 1).

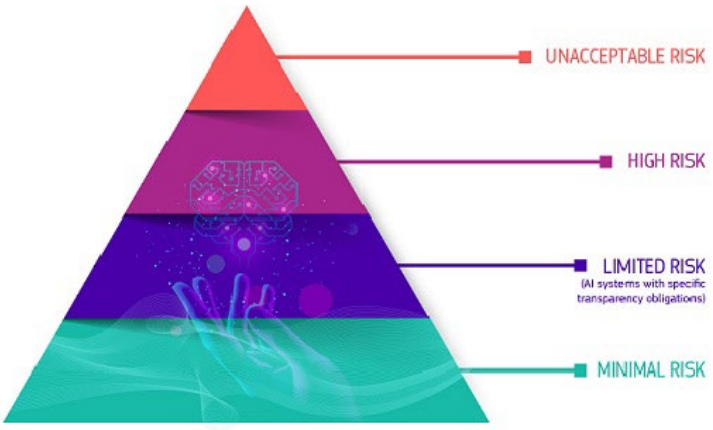

Fig. 1. La piramide del rischio dell'AI Act. Fonte: Commissione europea.

3.1. Le pratiche di IA vietate (art. 5, Cons. 28-44)

Alcune pratiche di IA sono vietate in quanto comportano un rischio inaccettabile per i diritti e libertà fondamentali.

È opportuno notare che il Regolamento fa riferimento a "pratiche", intendendo attività che possono essere svolte tramite i sistemi di intelligenza artificiale. Non è, quindi, il sistema in sé ad essere pericoloso, ma l'utilizzo dello stesso volto a realizzare una delle pratiche descritte.

I divieti di svolgere le pratiche di seguito descritte si applicano a decorrere dal **2 febbraio 2025**.

Tecniche subliminali e sfruttamento di vulnerabilità

È vietato utilizzare sistemi di IA al fine di distorcere materialmente il comportamento di una persona o di un gruppo di persone. Per rientrare nel divieto il sistema di IA deve:

- Usare tecniche subliminali senza che una persona ne sia consapevole, oppure
- Usare tecniche deliberatamente manipolative o ingannevoli.

Il divieto di queste pratiche mira a tutelare la libertà di autodeterminazione e il principio di trasparenza, analogamente a quanto già avviene nella tutela dei consumatori. Tuttavia, per applicare il divieto, occorre dimostrare non solo l'utilizzo di tecniche ingannevoli o subliminali, ma anche che queste influenzino il processo decisionale portando a scelte diverse e potenzialmente dannose, con effetti negativi rilevanti su salute fisica, psicologica o interessi finanziari. È interessante notare che la distorsione del comportamento può derivare anche da fattori esterni non controllabili dal fornitore o deployer del sistema AI, dato che la norma non richiede che il sistema sia intenzionalmente creato per produrre tali effetti.

Esempi di pratiche che rientrano in questo divieto possono essere servizi di streaming che inseriscono messaggi subliminali nei video o nei film, chatbot "sentimentali" che inducono in maniera manipolatoria a svolgere delle azioni che possono causare effetti dannosi sulla salute fisica, psicologica, o sugli interessi finanziari dell'utente.

Divieto di social scoring

Il divieto vuole impedire che vengano creati sistemi di social scoring, ossia sistemi che valutano o classificano le persone in base al comportamento sociale o caratteristiche personali assegnando loro un punteggio sociale che può determinare un trattamento pregiudizievole o sfavorevole in contesti sociali non collegati a quelli in cui i dati sono originariamente raccolti, oppure un trattamento pregiudizievole o sfavorevole che sia ingiustificato o sproporzionato rispetto al comportamento o alla gravità dello stesso.

Il divieto vuole evidentemente tutelare la dignità umana, il divieto di non discriminazione e il principio di uguaglianza.

Si tratta, evidentemente, di un divieto rivolto più all'autorità pubblica che ai privati, volto a tutelare i cittadini e le persone verso forme di controllo da parte dello Stato (l'esempio è il sistema utilizzando in Cina che, sulla base del comportamento mantenuto in determinati ambiti, assegna dei punteggi sociali che possono anche impedire di svolgere certe azioni ai cittadini (come richiedere un passaporto, frequentare certi istituti scolastici, etc.).

Giustizia predittiva

Il divieto di pratiche di IA previsto dall'art. 5, par. 1, lett. d) dell'AI Act, che trova fondamento nel principio della presunzione di innocenza come indicato dal Considerando n. 42, si inserisce in un contesto in cui si richiede che le persone siano sempre giudicate in base al loro effettivo comportamento. Il Regolamento pone l'accento sul fatto che il giudizio non possa basarsi esclusivamente sulla profilazione o su caratteristiche personali come la cittadinanza, il luogo di nascita o di residenza, il numero di figli, il livello di indebitamento o il tipo di automobile posseduta, ovvero su elementi che hanno scarsa attinenza con la condotta che il giudice è chiamato a valutare.

Il divieto non si applica ai sistemi utilizzati a supporto di una valutazione umana del coinvolgimento in un'attività criminosa, purché tale valutazione si fondi su fatti oggettivi e verificabili direttamente connessi all'attività stessa. In sintesi, l'AI Act proibisce sempre l'impiego di sistemi di IA per predire la commissione di un reato, mentre ne consente l'uso per valutare il coinvolgimento di un soggetto in un'attività criminosa sulla base di prove concrete, senza però valutarne la capacità a delinquere.

L'esempio più famoso è quello del software statunitense COMPAS che veniva utilizzato nelle corti statunitensi per valutare la possibilità di recidiva. E' emerso che il software forniva la valutazione probabilistica sulla base di fattori diversi ed esterni rispetto alla sola condotta ed alle caratteristiche dell'imputato (valutando anche amicizie, quartiere di residenza, etc.) risolvendosi in un software discriminatorio per le persone di colore. In verità, la Corte Suprema investita della tematica ha ritenuto lecito l'utilizzo del software in quanto "strumento di supporto" alla decisione del giudice.

Creazione di banche dati per il riconoscimento facciale con tecniche di scraping

L'uso di sistemi di IA per creare o espandere database di riconoscimento facciale, attraverso lo scraping di immagini online o da registrazioni di telecamere CCTV, alimenta il timore di una sorveglianza di massa e confligge con il diritto alla protezione dei dati personali. Di conseguenza, l'art. 5, par. 1, lett. e) dell'AI Act pone il divieto di tali pratiche.

Il caso più noto è quello della società Clearview, sanzionata anche dal Garante italiano, che aveva creato una banca dati svolgendo attività di scraping sui social network e delle riprese video delle telecamere a circuito chiuso al fine di consentire l'associazione dei volti delle persone.

Divieto di inferenza di emozioni

Il Considerando n. 44 precisa che i sistemi di IA per riconoscere le emozioni delle persone sarebbero ancora non affidabili, in quanto privi di specificità e limitati rispetto alla variabilità dell'espressione delle emozioni, che può differire molto a seconda delle culture e delle situazioni in cui si trovano le persone. In considerazione di tali caratteristiche queste tipologie di sistemi potrebbero rivelarsi discriminatori.

La norma, d'altro canto, non vieta l'utilizzo di tali tecniche in via generale, ma ne è vietato l'utilizzo nel luogo di lavoro e negli istituti di istruzione, in considerazione dello squilibrio di potere che è connaturato in tali contesti. Il divieto non si applica ove in tali ambiti il sistema di IA per il riconoscimento delle emozioni abbia finalità mediche o di sicurezza.

È opportuno evidenziare che al di fuori di tali ambiti, tali sistemi di IA sono comunque considerati sistemi a rischio elevato, esaminando caratteristiche biometriche, in forza del combinato disposto dell'art. 6, par. 2 e del par. 1, lett. c) dell'Allegato III.

Ad esempio potrebbe ricadere in tale divieto un sistema di IA volto a verificare, attraverso l'analisi delle espressioni del visto, le emozioni di studenti nel corso di una prova di esame, al fine di determinare se gli stessi

Classificazioni biometriche

L'utilizzo di dati biometrici di una persona (come, ad esempio, il volto o le impronte digitali) potrebbe consentire di categorizzare la stessa al fine di trarre deduzioni o inferenze in merito alle opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, razza, vita sessuale o orientamento sessuale.

L'art. 5, par. 1, lett. g) vieta tali pratiche, fatte salve le ipotesi in cui le classificazioni o il filtraggio sono svolti su dataset biometrici acquisiti legittimamente, come la selezione di immagini in base al colore dei capelli o degli occhi (Considerando n. 30).

Un esempio è la pratica posta in essere in Cina che, sistemi di intelligenza artificiale (inseriti nella IJOP - Integrated Joint Operation Platform), identifica e traccia gli appartenenti alla popolazione degli Uiguri anche sulla base di dati relativi alle caratteristiche somatiche.

Identificazione biometrica in tempo reale in spazi accessibili al pubblico

L'art. 5, par. 1, lett. h) dell'AI Act, frutto di un complesso processo di mediazione, disciplina l'uso dei sistemi di IA per il riconoscimento biometrico remoto in tempo reale in spazi pubblici da parte delle forze dell'ordine. Nonostante la proposta iniziale del Parlamento europeo di vietare completamente tali pratiche, ritenute particolarmente invasive per i diritti e le libertà individuali, il regolamento prevede tre eccezioni:

- il sistema è utilizzato per ricercare in maniera mirata specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, o persone scomparse;
- il sistema è volto a prevenire una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;
- il sistema è utilizzato per la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale relativamente ai reati di cui all'allegato II del Regolamento, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno 4 anni.

L'uso di questi sistemi in tali ipotesi è comunque soggetto a ulteriori condizioni, dato che comunque rientrano nei sistemi di IA a rischio elevato in quanto analizzano dati biometrici; sarà quindi necessario svolgere una valutazione d'impatto sui diritti fondamentali e registrare il sistema nella banca dati UE.

Inoltre, è richiesta un'autorizzazione preventiva da parte di un'autorità giudiziaria o amministrativa indipendente, salvo casi di urgenza.

Ogni Stato membro può autorizzare l'impiego di tali sistemi nel proprio territorio, nel rispetto dei vincoli del Regolamento, attraverso una normativa nazionale che specifichi finalità, reati ammessi, norme per le autorizzazioni e attività di verifica.

Infine, nessuna decisione con effetti negativi su una persona può basarsi unicamente sull'output del sistema di identificazione, richiedendo ulteriori elementi probatori.

Diversa la disciplina per i sistemi di IA di **identificazione biometrica remota a posteriori** (ossia non in tempo reale). Tali sistemi non rientrano nel divieto di cui all'art. 5, ma sono considerati sistemi di IA ad alto rischio ed oltre a dover rispettare i requisiti e le garanzie previste per tali sistemi, per il loro utilizzo di deployer osservare le previsioni di cui all'art. 26 dell'AI Act.

Le violazioni delle disposizioni riguardanti le pratiche di AI proibite sono punite con le sanzioni più severe (art. 99, par. 3) potendo arrivare le sanzioni amministrative a 35.000.000 di euro oppure, nel caso di imprese, al 7% del fatturato mondiale annuo dell'esercizio precedente, se superiore.

3.2. I sistemi di IA ad alto rischio (art. 6)

Per questi sistemi non vige un divieto assoluto di utilizzo, ma, in forza di una prevalutazione da parte del legislatore europeo, si ritiene che possano comportare un alto rischio per le persone, in particolare per i loro diritti fondamentali. La categorizzazione dei sistemi come ad alto rischio si basa, ai sensi dell'art. 6, sul rinvio agli Allegati I e III.

La categoria comprende due insiemi principali:

- sistemi che sono destinati ad essere utilizzati come **componente di sicurezza di un prodotto**, o il sistema di IA è esso stesso un prodotto, coperto dalla legislazione di armonizzazione dell'Unione elencata nell'Allegato I, oppure si tratti di un sistema che deve essere sottoposto a

valutazione di conformità da parte di terzi sempre sulla base della normativa di armonizzazione prevista in Allegato I[1] (par. 6, par. 1, Allegato I -art. 3, n. 14 – cons. 49-52);

- **i sistemi di IA che non sono componenti di altri prodotti individuati nell'Allegato III** con riferimento al loro utilizzo in determinati ambiti per il perseguimento di specifiche finalità. Si tratta:
    1. **identificazione e categorizzazione biometrica** delle persone o riconoscimento delle emozioni;
    2. **componenti di sicurezza nella gestione e funzionamento delle infrastrutture critiche** (infrastrutture digitali critiche, gestione del traffico stradale e fornitura di servizi essenziali quali acqua, gas, riscaldamento ed elettricità);
    3. **istruzione e formazione professionale**, per l'utilizzo ai fini dell'accesso, ammissione o per l'assegnazione a istituti di istruzione, nonché, più in generale, per la formazione professionale a tutti i livelli; per la valutazione dei risultati di apprendimento o per valutare l'adeguatezza del livello di istruzione che un individuo riceverà o sarà in grado di ricevere, sempre in ambito dell'istruzione e della formazione professionale; per monitorare e riconoscere comportamenti vietati durante le prove negli istituti e nella formazione professionale;
    4. **occupazione, gestione dei lavoratori e accesso al lavoro autonomo**, come i sistemi utilizzati per il recruiting o la selezione delle persone (anche in sede di pubblicazione di

[1] L'Allegato I contiene l'elenco della legislazione di armonizzazione e comprende il Regolamento macchine, le disposizioni sulla sicurezza dei giocattoli, le disposizioni su imbarcazioni da diporto e moto d'acqua, le norme di sicurezza su ascensori e componenti, gli apparecchi e sistemi di protezione destinati ad essere usati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, impianti a fune, disposizioni di protezione individuale, apparecchi che bruciano carburanti gassosi, dispositivi medici, dispositivi medico-diagnostici in vitro. L'elenco degli altri atti legislativi di armonizzazione comprende: il Regolamento sulla sicurezza dell'aviazione civile, il Regolamento sull'omologazione dei veicoli a due ruote, tre ruote o quadricicli, il Regolamento sui veicoli agricoli e forestali, la Direttiva sull'equipaggiamento marittimo, la Direttiva sull'interoperabilità del sistema ferroviario, i regolamenti sui veicoli a motore e loro rimorchi, il Regolamento sugli aereomobili, anche senza pilota.

annunci mirati, analisi e selezione delle domande e valutazione dei candidati); per assumere decisioni inerenti la promozione dei dipendenti o la cessazione del rapporto, assegnazione di mansioni sulla base del comportamento individuale, per il monitoraggio e la valutazione delle prestazioni o del comportamento;

5. **accesso a prestazioni e servizi essenziali e fruizione degli stessi,** che comprendono: a) sistemi di IA utilizzati dalle amministrazioni pubbliche o per loro conto, per valutare l'ammissibilità a prestazioni di assistenza pubblica essenziale, comprensive dei servizi sanitari e la gestione di tali servizi; b) utilizzati da chiunque per la valutazione del merito creditizio o per stabilire l'affidabilità delle persone fisiche, ad eccezione dei sistemi antifrode; c) sistemi per la valutazione del rischio o la determinazione dei premi per le assicurazioni vita e malattia; d) sistemi utilizzati nei servizi di pronto intervento, polizia, vigili del fuoco, assistenza medica, per classificare le chiamate di emergenza, per inviare i servizi di emergenza, e nel settore sanitario quelli per stabilire la selezione dei pazienti in caso di assistenza di emergenza;
6. **attività di contrasto**, comprendente i sistemi IA utilizzati per valutare il rischio che una persona fisica diventi vittima di reati; quelli a sostegno delle autorità di contrasto come poligrafi o strumenti simili, quelli utilizzati per valutare l'affidabilità delle prove nel corso di indagini o azioni penali; i sistemi IA utilizzati per valutare il rischio di commissione di reato o di recidiva; i sistemi utilizzati per la profilazione delle persone fisiche nel corso dell'accertamento, indagini e perseguimento di reati;
7. **gestione della migrazione**, **dell'asilo e del controllo delle frontiere**, ossia i sistemi di IA utilizzati dalle autorità pubbliche competenti o per loro conto, o da istituzioni, organi e organismi dell'Unione, quali poligrafi o simili su persone che intendono entrare o sono entrate nel territorio di uno Stato al fine di una valutazione di rischio, compreso un rischio di sicurezza, un rischio di migrazione irregolare o un rischio sanitario; sistemi di ausilio all'esame delle domande di asilo, visto e permesso di

soggiorno e dei relativi reclami; sistemi utilizzati nel contesto della gestione della migrazione, dell'asilo e del controllo di frontiera, per rilevare, riconoscere o identificare persone fisiche (ad eccezione dei documenti di viaggio);

8. **amministrazione della giustizia e processi democratici** per i sistemi di IA utilizzati dall'autorità giudiziaria, o per suo conto, nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie di fatti; sistemi utilizzati per influenzare l'esito di un'elezione, di un referendum o il comportamento di voto delle persone, ad esclusione dei sistemi per organizzare, ottimizzare e strutturare le campagne politiche dal punto di vista amministrativo e logistico.

Mentre il primo insieme di sistemi di AI ad alto rischio tramite rinvio alla normativa di armonizzazione di cui all'Allegato I costituisce la conseguenza di trattare l'intelligenza artificiale come prodotto, considerando quindi ad alto rischio tutti i sistemi AI che ricadono nei settori merceologici in cui è intervenuta una norma armonizzata di sicurezza, l'individuazione dei sistemi ad alto rischio tramite il rinvio all'Allegato III è frutto delle analisi e delle salvaguardie relative ai rischi sui diritti fondamentali delle persone che i sistemi IA potrebbero far sorgere, con una scelta incentrata più sui potenziali effetti negativi che il loro utilizzo potrebbe comportare.

L'utilizzo di un sistema di IA nell'ambito di uno dei settori e per le casistiche individuate nell'Allegato III non sempre comporta la sua collocazione tra i sistemi a rischio elevato.

Il par. 3 dell'art. 6 prevede che un sistema di IA può essere escluso dalla categoria ad alto rischio se non presenta un rischio significativo per la salute, la sicurezza o i diritti fondamentali delle persone e non influenza in modo sostanziale il risultato del processo decisionale.

Questo avviene quando il sistema svolge un compito procedurale limitato, migliora il risultato di un'attività umana già completata, rileva schemi decisionali senza sostituire la valutazione umana, o esegue un compito preparatorio per i casi d'uso dell'allegato III.

Tuttavia, anche se soddisfa queste condizioni, un sistema di AI sarà sempre considerato ad alto rischio se effettua una profilazione di persone fisiche.

Il fornitore, qualora ritenga che il sistema di IA di cui all'allegato III non sia ad alto rischio dovrà documentare tale valutazione prima della sua messa in servizio o immissione sul mercato, con obbligo di mettere a disposizione tale documentazione alle autorità nazionali di controllo e di registrarsi nella banca dati UE.

I requisiti e gli obblighi sugli operatori che immettono, mettono in servizio o usano nel mercato europeo sistemi di AI ad alto rischio si applicheranno decorsi 3 anni (per i sistemi compresi nell'Allegato I) o 2 anni (per i sistemi compresi nell'Allegato III) dalla data di entrata in vigore dell'AI Act, quindi, rispettivamente, dal 2 agosto 2027 e dal 2 agosto 2026 (art. 113, par. 3, lett. c) e par. 2).

Un regime transitorio è previsto dall'art. 111, par. 2 per i sistemi AI ad alto rischio già presenti sul mercato.

3.2.1. I requisiti di conformità dei sistemi di IA ad alto rischio

L'AI Act prevede una certa flessibilità per determinare e adattare gli obblighi relativi ai sistemi di IA ad alto rischio, riconoscendo la diversità degli operatori coinvolti e dei contesti di utilizzo. Gli obblighi, infatti, sono assegnati in modo proporzionale al ruolo degli operatori nella catena del valore: i fornitori devono garantire la conformità tecnica e documentale dei sistemi, mentre i deployer sono obbligati a monitorare l'uso del sistema, segnalare malfunzionamenti e attenersi alle istruzioni del fornitore.

Peraltro, in molti casi, è consentito ricorrere alla auto-valutazione del sistema da parte del fornitore, per decidere se il sistema soddisfa i criteri di "alto rischio". I fornitori possono esentare alcune applicazioni di IA dalle regole stringenti se: a) sono destinate esclusivamente alla ricerca e sviluppo e b) vengono utilizzate in contesti sperimentali (es. sandbox normative).

Le PMI e le start-up possono beneficiare di agevolazioni quali la riduzione degli oneri documentali e l'accesso a programmi di supporto tecnico e finanziario.

3.2.2. Requisiti obbligatori relativi ai sistemi di IA ad alto rischio (art. 8-15, Cons. 46, Cons. 59-78)

I requisiti di conformità dei sistemi di IA ad alto rischio sono individuati in modo dettagliato e posti a **carico del fornitore** con l'obbligo di assicurarne l'efficace attuazione. I requisiti coprono tutto il ciclo di vita del sistema, dalla progettazione all'utilizzo e segnatamente:

- **sistema di gestione dei rischi lungo l'intero ciclo di vita del sistema di IA**. Il sistema di gestione dei rischi per i sistemi di AI ad alto rischio è un processo iterativo continuo che copre l'intero ciclo di vita del sistema, comprendente l'identificazione, l'analisi, la stima e la valutazione dei rischi noti e prevedibili, emergenti e derivanti dal monitoraggio post-immissione sul mercato. Le misure di gestione dei rischi, che tengono conto degli effetti combinati dei requisiti previsti, includono l'eliminazione o la riduzione dei rischi attraverso un'adeguata progettazione e fabbricazione, l'attuazione di misure di attenuazione e controllo, e la fornitura di informazioni e formazione ai deployer. I sistemi devono essere sottoposti a prove per individuare le misure più appropriate, prestando attenzione all'eventuale impatto negativo su minori o altri gruppi vulnerabili;
- **requisiti per la qualità dei dataset di addestramento**. L'art. 10 dell'AI Act stabilisce che i sistemi di IA ad alto rischio che utilizzano tecniche di addestramento di modelli devono essere sviluppati sulla base di set di dati che soddisfano specifici criteri di qualità e sono soggetti a pratiche di governance e gestione adeguate. Tali set di dati devono essere pertinenti, rappresentativi, esenti da errori e completi, possedendo appropriate proprietà statistiche anche in relazione alle persone o gruppi a cui il sistema è destinato, al fine di evitare bias in fase di addestramento. L'articolo consente eccezionalmente, se strettamente necessario per garantire il rilevamento e la correzione delle distorsioni, l'utilizzo di categorie particolari di dati personali (dati sensibili), nel rispetto di specifiche condizioni e tutele.
- **predisposizione di idonea documentazione tecnica**. L'art. 11 dell'AI Act prevede che la documentazione tecnica relativa ai sistemi di AI ad alto rischio debba essere redatta prima dell'immissione sul mercato o della messa in servizio e tenuta aggiornata. Tale documentazione deve dimostrare la conformità del sistema ai requisiti previsti, fornendo alle

Autorità competenti e agli organismi notificati le informazioni necessarie per valutare tale conformità, e contenere almeno gli elementi elencati nell'allegato IV del Regolamento. Per agevolare le PMI e le start-up, è prevista la possibilità di fornire in modo semplificato gli elementi della documentazione tecnica utilizzando un apposito modulo che sarà definito dalla Commissione. Nel caso di sistemi di IA connessi a prodotti disciplinati da altra normativa di armonizzazione UE, deve essere redatta un'unica documentazione tecnica contenente tutte le informazioni richieste.

- **messa in opera di un sistema per la registrazione delle operazioni (logging) effettuate dal sistema di IA.** L'art. 12 del Regolamento UE 2024/1689 impone ai fornitori di sistemi di AI ad alto rischio di registrare automaticamente gli eventi per l'intero ciclo di vita, al fine di tracciare situazioni di rischio, di eseguire il monitoraggio post-immissione sul mercato e verificare il funzionamento del sistema. I sistemi di identificazione biometrica devono mantenere registrazioni specifiche, includendo anche il periodo di utilizzo, la banca dati di riferimento utilizzata per verificare i dati di input e gli identificativi delle persone coinvolte nella verifica dei risultati;
- **trasparenza by design e predisposizione di specifiche istruzioni.** I sistemi di IA ad alto rischio devono essere progettati e sviluppati in modo da garantire un livello di trasparenza adeguato, consentendo ai deployer di interpretare e utilizzare correttamente l'output del sistema. I sistemi devono essere accompagnati da istruzioni per l'uso per consentire al deployer di comprendere il funzionamento del sistema. Esse devono includere, tra l'altro, l'identità e i contatti del fornitore, le caratteristiche, capacità e limiti del sistema, le misure di sorveglianza umana, le risorse computazionali e hardware necessarie e meccanismi per consentire ai deployer di raccogliere, conservare e interpretare correttamente i log, ove previsto;
- **introduzione di sistemi che consentano la supervisione umana (human oversight**). Deve essere consentita una supervisione da parte di persone fisiche durante l'utilizzo dei sistemi di IA ad alto rischio, ciò in misura proporzionata ai rischi, al livello di autonomia e al contesto di utilizzo del sistema, e le misure per consentire tale supervisione possono essere integrate nel sistema dal fornitore o

individuate dal fornitore per essere attuate dal deployer. Per i sistemi di AI ad alto rischio che effettuano riconoscimento biometrico, le misure devono garantire che il deployer non compia azioni o adotti decisioni basate sull'identificazione risultante dal sistema, a meno che non vi sia stata una verifica e conferma separata da almeno due persone fisiche autorizzate, salvo che il sistema sia utilizzato per finalità di contrasto, migrazione, controllo delle frontiere o asilo, sulla base di una valutazione di proporzionalità prevista dal diritto dell'Unione o nazionale;

- **requisiti in termini di accuratezza, robustezza e cybersicurezza.** I sistemi di IA ad alto rischio devono garantire accuratezza, robustezza e cybersicurezza durante l'intero ciclo di vita, con livelli adeguati che vanno documentati e misurati secondo parametri di riferimento e metodologie di misurazione stabiliti dalla Commissione Europea in collaborazione con gli stakeholder. I sistemi devono implementare misure tecniche e organizzative, inclusi meccanismi di backup e *fail-safe*, per massimizzare la resilienza contro errori, malfunzionamenti e attacchi esterni che potrebbero sfruttarne le vulnerabilità.

3.2.3. Altri obblighi posti a carico del fornitore (art. 16-22, Cons. 79-82)

Oltre ai requisiti specifici per i sistemi di IA ad alto rischio, l'AI Act impone **obblighi aggiuntivi ai fornitori** per garantire una gestione responsabile dei sistemi IA durante tutto il loro ciclo di vita. Si tratta di obblighi che riguardano aspetti operativi, gestionali e di trasparenza e sono relativi a: sistema di gestione della qualità, aggiornamenti e manutenzione, registrazione del sistema nella banca dati, segnalazione di incidenti e anomalie, collaborazione con le autorità, ecc.

Nel dettaglio (art. 16):

- indicazione dei riferimenti del fornitore, mediante l'apposizione del nome o marchio sul sistema o sulla documentazione di accompagnamento;
- istituire e documentare un sistema di gestione della qualità, con le caratteristiche che sono state già riassunte al paragrafo precedente;

- conservare la documentazione tecnica relativa al sistema di IA, che deve poter essere messa a disposizione a richiesta delle Autorità per un periodo di 10 anni dall'immissione sul mercato/ messa in servizio del sistema di IA;
- per un periodo minimo di 6 mesi, salvo eventuali diversi periodi di tempo stabiliti dal diritto unionale o nazionale applicabile, conservare i log generati dal sistema di IA ad alto rischio;
- sottoporre il sistema alla procedura di valutazione della conformità, redigere una dichiarazione di conformità UE ed apporre la marcatura CE. L'obbligo di svolgere la valutazione di conformità è il punto centrale della normativa di prodotto, e il Regolamento la disciplina in maniera differenziata. Essa è sempre obbligatoria per i sistemi di IA ad alto rischio, ma è disciplinata in maniera differente a seconda dell'applicazione o meno di norme standardizzate e della tipologia di sistemi di IA (ad alto rischio o eccezione di una pratica vietata), distinzione che si riflette anche sulla necessità di coinvolgere o meno un organismo di valutazione esterno. Anche l'esistenza o meno delle norme di armonizzazione (che devono essere adottate dagli organismi di standardizzazione europei CEN, CENELEC, ETSI) incide sull'estensione dell'obbligo, in quanto l'adesione a tali norme fonda una presunzione di conformità del sistema di IA. L'esito positivo della valutazione di conformità consente di apporre il marchio CE al momento dell'immissione sul mercato (o messa in servizio), che potrà essere apposto anche sulla sola documentazione di accompagnamento. La dichiarazione di conformità deve essere conservata per 10 anni dall'immissione sul mercato o messa in servizio, in quanto richiedibili in tale lasso di tempo dalle Autorità di controllo;
- registrarsi e registrare il sistema di IA nella banca dati UE;
- adottare le misure correttive necessarie qualora un sistema di IA ad alto rischio non sia conforme al Regolamento, dovendo anche, a seconda dei casi, ritirarlo, disabilitarlo o richiamarlo. In presenza di incidenti gravi il fornitore dovrà attivarsi immediatamente e informare l'Autorità di controllo;
- garantire che il sistema di IA sia conforme ai requisiti di accessibilità di cui alle Direttive (UE) 2016/2012 e (UE) 2019/882;

- se necessario nominare, mediante mandato scritto, un rappresentante autorizzato stabilito nell'UE;
- monitorare il sistema di IA ad alto rischio successivamente alla sua immissione sul mercato.

3.2.4. Obblighi a carico del deployer (art. 26, Cons. 93)

Il Regolamento impone anche **obblighi specifici ai deployer** (coloro che utilizzano i sistemi di IA ad alto rischio nell'ambito della loro attività professionale). Si tratta di obblighi che si concentrano sul monitoraggio, sulla trasparenza e sulla gestione dei rischi durante l'uso del sistema.

I deployer, infatti, diversamente dai fornitori, non sono soggetti a un obbligo generale di compliance come quello previsto dall'articolo 16. Il loro dovere principale si limita invece a garantire, attraverso l'adozione di misure sia tecniche sia organizzative, che il sistema di IA venga utilizzato in modo appropriato e in conformità con le istruzioni d'uso fornite con il sistema stesso.

L'AI Act richiede al deployer di dotarsi di un **livello adeguato di alfabetizzazione** in materia di IA e gli impone di:

- adottare idonee misure tecniche e organizzative;
- affidare la sorveglianza umana a persone fisiche che dispongano della competenza, della formazione, dell'autorità e del sostegno necessari;
- garantire che i dati di input, qualora il deployer ne abbia il controllo, siano pertinenti e sufficientemente rappresentativi secondo la finalità prevista del sistema di IA;
- monitorare il funzionamento dei sistemi di IA ad alto rischio dopo la loro immissione sul mercato, basandosi sul sistema di monitoraggio predisposto dal fornitore secondo l'articolo 72. Tale monitoraggio comporta due obblighi specifici: informare il fornitore dell'attività di monitoraggio svolta e, qualora emerga che l'uso del sistema secondo le istruzioni possa mettere a rischio salute, sicurezza o diritti fondamentali delle persone, informare immediatamente il fornitore, il distributore e l'Autorità di vigilanza del mercato, sospendendo contemporaneamente l'utilizzo del sistema;

- conservare, per un periodo di almeno 6 mesi, salvo diverse disposizioni dell'ordinamento nazionale, i log generati automaticamente dal sistema qualora nella propria disponibilità;
- informare le rappresentanze dei lavoratori e i lavoratori medesimi dell'utilizzo di un sistema di IA ad alto rischio, norma che dovrà essere coordinata con il D.Lgs. n. 104/2022 (Decreto Trasparenza). Un obbligo di trasparenza in capo ai deployer è stabilito anche per le persone che possono essere soggette all'uso di sistemi di IA ad alto rischio volti ad adottare decisioni o assistere l'adozione di decisioni che riguardano tali persone;
- i deployer che sono Autorità pubbliche o pubbliche amministrazioni devono registrarsi nella banca dati UE, selezionando il sistema di IA ad alto rischio utilizzao e registrandone il relativo uso.

I deployer devono poi collaborare con le Autorità di controllo in caso di verifiche o richieste di informazioni sui sistemi di IA ad alto rischio utilizzati.

3.2.5. Quali deployer devono eseguire la valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio (Fundamental Rights Impact Assessment - FRIA) (art. 27, Cons. 96)

L'AI Act prevede un obbligo specifico per particolari categorie di deployer, ossia i deployer dei sistemi di IA ad alto rischio di cui all'Allegato III (ad eccezione di quelli riguardanti la gestione e il funzionamento di infrastrutture critiche) che sono organismi di diritto pubblico o enti privati che forniscono servizi pubblici, nonché per tutti i deployer di sistemi ad alto rischio utilizzati nell'ambito della valutazione dell'affidabilità creditizia delle persone fisiche e per quelli utilizzati per la valutazione dei rischi e la determinazione dei prezzi nel ramo delle assicurazioni vita e sanitarie.

I deployer sopra indicati devono effettuare una valutazione dell'impatto sui diritti fondamentali.

La Fundamental Rights Impact Assessment (FRIA) è una valutazione di impatto finalizzata a: a) identificare rischi specifici sui diritti fondamentali di individui o gruppi coinvolti nell'utilizzo di sistemi di IA ad alto rischio e b) definire le relative contromisure.

La valutazione prevede una descrizione dettagliata dei processi di utilizzo del sistema, delle tempistiche previste, delle categorie di persone interessate e dei potenziali rischi, coinvolgendo anche stakeholder pertinenti come rappresentanti dei gruppi impattati, esperti indipendenti e organizzazioni della società civile. La FRIA deve inoltre includere le misure di sorveglianza umana, le strategie di gestione del rischio e i meccanismi di reclamo.

La FRIA deve essere aggiornata quando si modificano gli elementi in essa contenuti e va effettuata prima della messa in uso del sistema, potendo basarsi su valutazioni precedenti in casi analoghi o su quelle del fornitore.

L'AI Act prevede un'integrazione con la DPIA del GDPR per evitare duplicazioni, concentrandosi sui diritti fondamentali diversi dalla protezione dei dati personali.

È inoltre previsto che l'Ufficio per l'IA fornisca un modello di questionario per facilitare i deployer nell'adempimento degli obblighi, inclusa la notifica dell'avvenuta FRIA all'Autorità di vigilanza sul mercato, salvo deroghe autorizzate.

3.2.6. Obblighi degli altri operatori dell'AI Value Chain

L'AI Act attribuisce infine specifici obblighi anche agli altri operatori coinvolti nella catena del valore dei sistemi di IA ad alto rischio, oltre a fornitori e deployer. Sono operatori che includono importatori, distributori, fabbricanti di prodotti integrati e rappresentanti autorizzati, con l'obiettivo di garantire la conformità normativa lungo tutta la filiera.

Gli **importatori,** cioè chi introduce sistemi di IA sviluppati fuori dall'UE nel mercato europeo, devono verificare che il sistema sia conforme alle norme europee prima dell'immissione sul mercato, assicurarsi che il fornitore abbia redatto la documentazione tecnica e adempiuto agli obblighi di registrazione, conservare una copia della dichiarazione di conformità e metterla a disposizione delle autorità competenti su richiesta.

I **distributori**, cioè chi rende disponibili i sistemi di IA sul mercato UE senza esserne il fornitore o l'importatore, devono garantire che il sistema sia accompagnato da tutte le informazioni e istruzioni predisposte dal fornitore, non commercializzare sistemi di IA che non soddisfano i requisiti normativi,

informare il fornitore e le Autorità competenti di eventuali rischi o problemi riscontrati.

I **fabbricanti di prodotti** che includono sistemi di IA ad alto rischio sono considerati fornitori del sistema IA e devono assicurarsi che il sistema di IA sia conforme ai requisiti del Regolamento, garantendo che l'integrazione del sistema IA nel prodotto non comprometta la sicurezza o la conformità normativa.

I **rappresentanti autorizzati**, la cui nomina è obbligatoria per i fornitori non stabiliti nell'UE, agiscono in nome di questi e garantiscono la conformità normativa del sistema di IA. Il rappresentante deve essere situato nell'UE, mantenere la documentazione tecnica e cooperare con le Autorità competenti per eventuali controlli o indagini.

I **fornitori di componenti o strumenti o servizi** dei sistemi di IA ad alto rischio devono garantire che tali elementi soddisfino i requisiti tecnici e di sicurezza nonché mettere a disposizione del fornitore tutte le informazioni necessarie per assicurare la conformità complessiva del sistema IA.

4. Obblighi di trasparenza (art. 50, Cons. 70, 71, 72)

Per i sistemi di IA progettati per interagire con le persone, il Regolamento stabilisce dei requisiti di trasparenza, al fine di scongiurare il rischio che l'utente non riconosca di interagire con un sistema di IA o non comprenda la natura artificiale dei contenuti prodotti da tale sistema ed eventualmente utilizzati.

Mentre inizialmente il Regolamento prevedeva solo obblighi di trasparenza per questi sistemi, il voto parlamentare del giugno 2023 ha introdotto sostanziali modifiche, includendo nuove definizioni e disposizioni specifiche per i modelli fondazionali, in risposta alla diffusione dell'IA generativa basata sui transformers.

Il Parlamento europeo inserendo due nuove definizioni ("sistemi di IA per scopi generali" (GenAI o GPAI) e i "modelli di IA per scopi generali") ha ampliato significativamente la portata dell'AI Act, estendendo la regolamentazione non solo alle applicazioni downstream, ma anche alla parte upstream della tecnologia, volendo introdurre maggiori tutele per la "libertà cognitiva" delle persone di fronte ai potenziali usi manipolatori e decettivi di questi sistemi.

L'articolo 50 del Regolamento stabilisce un obbligo di trasparenza per i sistemi di IA che interagiscono direttamente con le persone fisiche, al fine di contrastare rischi di impersonificazione e inganni. Tale obbligo richiede una "trasparenza by design", per cui i sistemi devono essere progettati e sviluppati in modo da informare gli utenti che stanno interagendo con un'IA e può essere derogato solo quando l'interazione con un sistema di IA sia già evidente per una persona fisica ragionevolmente informata, attenta e avveduta.

Le informazioni devono essere date in modo chiaro e distinguibile, al più tardi al momento della prima interazione o esposizione della persona con il sistema di IA.

I sistemi di IA che rientrano nelle previsioni di trasparenza sono (art. 50):

- sistemi di IA destinati a interagire direttamente con le persone fisiche;
- sistemi di IA, compresi sistemi con finalità generali (GPAI), che generano contenuti audio, immagini, video o testuali sintetici. In tale ipotesi è previsto che il fornitore provveda affinché i contenuti vengano contrassegnati in formato leggibile dalla macchina e rilevabili come generati e manipolati artificialmente (*watermarking*), salvo per i sistemi

che assistono nell'editing standard o non alterano in modo sostanziale i dati di input o la rispettiva semantica;

- sistemi di riconoscimento delle emozioni o di categorizzazione biometrica. Per tali sistemi è previsto un obbligo del deployer di rispettare le norme in materia di protezione dei dati personali e informare le persone relativamente all'esposizione e funzionamento del sistema, salvo il caso in cui siano utilizzati per attività di contrasto;
- sistemi di IA che generano o manipolano immagini o contenuti audio o video che costituiscono un "deep fake" (ossia che assomigliano a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbero falsamente autentici o veritieri ad una persona). In tali casi i deployer devono rendere noto che il contenuto è stato generato o manipolato artificialmente, salvo l'uso per attività di contrasto dei reati e la cd. eccezione artistica, che si ha quando il contenuto faccia parte di un'analoga opera o di un programma manifestamente artistico, creativo, satirico o fittizio;
- sistemi di IA che generano o manipolano testo che è stato pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico, con obbligo di rendere noto che il testo è generato o manipolato artificialmente. Per tali utilizzi l'obbligo non si applica se il contenuto generato dall'AI è stato sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica detiene la responsabilità editoriale dello stesso.

5. Gli obblighi relativi ai modelli GPAI (General Purpose AI) (art. 3, n. 63, Cons. 97, art. 3, n. 68)

L'AI Act introduce obblighi specifici per i modelli di IA per finalità generali (GPAI), noti anche come **modelli fondazionali (foundation models)**, che sono ampiamente utilizzabili in molteplici contesti e applicazioni. Tali modelli, per la loro flessibilità e generalità, sono soggetti a requisiti che tengono conto della loro vasta gamma di utilizzi potenziali.

I modelli GPAI, infatti, sono caratterizzati da significativa generalità e capacità di svolgere con competenza un'ampia gamma di compiti distinti e per questo idonei a essere integrati in una serie di sistemi di IA 'a valle'.

5.1 Gli obblighi specifici per i fornitori di modelli GPAI

Il Regolamento prevede una serie di obblighi documentali e informativi per garantire trasparenza e tracciabilità:

- redigere e mantenere aggiornata la documentazione tecnica del modello GPAI, comprensiva di informazioni sul processo di addestramento e test ed i risultati della sua valutazione, nonché le informazioni di cui all'Allegato XI;
- predisporre, aggiornare e mettere a disposizione dei fornitori di sistemi di IA a valle informazioni e documentazione in modo che possano avere una buona comprensione delle capacità e dei limiti del modello, al fine di consentire a chi integra i modelli nei propri sistemi di rendere le dovute informazioni. L'elenco delle informazioni da fornire è contenuto nell'Allegato XII del Regolamento;
- attuare una politica per il rispetto del diritto d'autore e dei diritti connessi, con specifico riferimento alla previsione di cui all'art. 4, par. 3 della Direttiva n. UE 2019/790 (la cd. eccezione per il *text and data mining* applicabile a condizione che il titolare dei diritti non abbia espresso una riserva di utilizzo tramite un meccanismo di opt-out. Il tema è direttamente collegato all'utilizzo di meccanismi di web scraping per raccogliere dati da utilizzare per l'addestramento dei modelli di IA);

- redigere e mettere a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello GPAI secondo un template predisposto dall'Ufficio per l'IA;
- se necessario, nominare mediante mandato scritto un rappresentante autorizzato stabilito nell'Unione.

I primi due obblighi non si applicano ai fornitori di modelli GPAI rilasciati con licenza libera e open source (per i quali devono essere resi pubblici i parametri, i pesi, le informazioni sull'architettura e le informazioni sull'uso del modello), fatto salvo che si tratti di modelli GPAI a rischio sistemico.

I fornitori dei modelli di GenAI possono basarsi sui codici di buone pratiche, che devono essere adottati entro il 2 maggio 2025, al fine di dimostrare la loro conformità agli obblighi stabiliti dall'AI Act a loro carico, ciò fino alla pubblicazione di una norma armonizzata, la cui adesione fa scattare una presunzione di conformità.

5.2 Gli obblighi relativi ai modelli GPAI a rischio sistemico (art. 3, n. 65, artt. 51 e 52, Cons. 111-112-113)

L'AI Act introduce il concetto di "rischio sistemico" per i modelli a scopi generali, seguendo l'approccio del Digital Service Act (DSA). Secondo l'articolo 3, paragrafo 65, questo rischio si configura quando un modello di IA per finalità generali può avere un impatto significativo sul mercato dell'Unione, con potenziali effetti negativi su salute pubblica, sicurezza, diritti fondamentali o società che possono propagarsi lungo la catena del valore.

Il regolamento stabilisce un'interazione con il DSA: quando un modello GenAI è integrato in una piattaforma o motore di ricerca molto grande (VLOP o VLOSE), gli obblighi di gestione del rischio previsti dal DSA soddisfano anche quelli dell'AI Act. Tuttavia, se emergono rischi significativi specifici come definiti dall'AI Act, questi soggetti dovranno valutare anche tali rischi sistemici in aggiunta a quelli previsti dal DSA.

L'AI Act classifica come modelli GPAI sistemici quelli che ricadono in una delle seguenti situazioni:

- il modello ha elevate capacità di impatto valutate sulla base di strumenti e metodologie tecniche adeguate, compresi indicatori e parametri di

riferimento (che dovranno essere definiti con atti delegati della Commissione Europea);

- sono designati come tali da una decisione della Commissione, tenuto conto dei criteri di cui all'Allegato XIII, che mantiene un elenco dei modelli GPAI con rischio sistemico.

Un modello GPAI viene presunto con capacità di impatto elevato quando la quantità cumulativa di calcolo utilizzata per il suo addestramento supera il valore di 10^{25} operazioni in virgola mobile.

Gli obblighi specifici, in aggiunta agli obblighi previsti per i modelli GPAI di cui ai artt. 53 e 54, per i modelli GPAI sistemici sono (art. 55):

- effettuare una valutazione dei modelli in conformità a protocolli e strumenti standardizzati, al fine di identificare e mitigare il rischio sistemico, anche svolgendo e documentando degli *adversarial testing*;
- valutare e mitigare i rischi sistemici a livello UE, comprese le loro fonti, che possono derivare dall'immissione sul mercato o dall'uso di tali modelli (alcune misure sono indicate nel Considerando 114, tra cui politiche di gestione dei rischi, con processi di responsabilità e *governance*, monitoraggio successivo, misure durante il ciclo di vita del modello e cooperazione con i vari attori coinvolti nella *value chain*);
- in analogia a quanto previsto dall'art. 73 dell'AI Act, tenere traccia, documentare e riferire senza indebiti ritardi all'Ufficio per l'IA e, se del caso, alle Autorità nazionali competenti, le informazioni sugli incidenti gravi e le possibili misure correttive per affrontarli;
- garantire un livello adeguato di sicurezza informatica sia del modello sia della sua infrastruttura fisica.

In modo simile a quanto stabilito per i modelli di IA con finalità generali, i fornitori di modelli a rischio sistemico possono dimostrare la loro conformità agli obblighi dell'articolo 55 attraverso l'adozione di codici di condotta, in attesa della pubblicazione di uno standard armonizzato. Se non aderiscono a questi codici o non applicano lo standard armonizzato, che garantirebbero una presunzione di conformità, dovranno dimostrare il rispetto degli obblighi attraverso metodi alternativi.

6. Gli spazi di sperimentazione normativa (artt. 57-59, Cons. 138-147)

L'AI Act prevede l'istituzione di spazi di sperimentazione normativa (regulatory sandboxes), progettati per promuovere l'innovazione consentendo la sperimentazione di nuove tecnologie di IA in un ambiente regolamentato ma flessibile.

Si tratta di soluzioni che consentono di testare sistemi di IA innovativi in un ambiente controllato, agevolandone lo sviluppo, l'addestramento, la sperimentazione (anche in condizioni reali, se necessario) e la convalida, per un periodo definito, prima della loro immissione sul mercato.

Il processo avviene sotto la supervisione delle Autorità nazionali competenti, con il supporto delle Autorità garanti per la protezione dei dati.

Le regulatory sandboxes hanno lo scopo di mitigare i rischi, in quanto consentono di identificare e affrontare eventuali problematiche di conformità o sicurezza prima che i sistemi vengano immessi sul mercato. Inoltre, garantiscono la protezione dei diritti fondamentali durante la sperimentazione.

La partecipazione alle sandbox regolatorie, inoltre, consente di semplificare il rilascio delle valutazioni di conformità e prevede regimi agevolativi per le PMI europee.

6.1. Le caratteristiche e gli ambiti di applicazione degli spazi di sperimentazione

Le caratteristiche principali sono:

- **ambiente regolamentato**: le sandboxes sono supervisionate dalle Autorità nazionali competenti per la vigilanza sul mercato;
- **partecipazione facilitata**: particolare attenzione è data a start-up, PMI e progetti di ricerca, con il fine di ridurre barriere economiche e burocratiche;
- **temporaneità**: le sperimentazioni sono limitate nel tempo e finalizzate ad agevolare l'immissione sul mercato di sistemi di IA da parte dei partecipanti nonché ad ottenere informazioni utili per l'Autorità ai fini dell'applicazione della normativa.

7. GOVERNANCE E APPLICAZIONE: L'ASSETTO MULTILIVELLO DELL'AI ACT

L'AI Act istituisce un sistema di governance ed *enforcement* a due livelli, coinvolgendo organismi europei e nazionali per garantire un'applicazione uniforme e coordinata delle norme.

Livello UE: che si concentra sulla definizione delle regole, il monitoraggio e il coordinamento transnazionale, garantendo che il Regolamento sia applicato in modo coerente e che i sistemi IA rispettino gli standard di sicurezza e affidabilità. Ciò comporta:

- coordinamento centrale e definizione delle linee guida generali;
- monitoraggio dell'applicazione del Regolamento nei vari Stati membri;
- vigilanza affidata alla Commissione Europea sui fornitori di modelli di IA per finalità generali.

Livello nazionale: in cui le Autorità nazionali competenti sono responsabili dell'implementazione pratica del Regolamento nei singoli Stati membri, agendo come garanti della conformità e del rispetto delle norme a livello locale. Ciò comporta:

- implementazione delle regole sul territorio,
- sorveglianza e controllo dei sistemi IA immessi sul mercato o utilizzati.

7.1. Organismi che operano a livello UE

L'Ufficio per l'IA esercita i compiti di vigilanza assegnati alla Commissione Europea, nonché compiti di monitoraggio, attuazione del Regolamento e supervisione dei sistemi IA ad alto rischio, dei modelli di IA per finalità generali e riceve gli eventuali reclami che possono essere presentati dai "fornitori a valle" di un sistema IA per scopi generali.

Il Consiglio per l'IA europeo (*European Artificial Intelligence Board* – EAIB), costituito da un membro per ogni Stato membro, che deve possedere adeguate competenze e autorità per eseguire le mansioni assegnate. Il Consiglio include due gruppi permanenti dedicati a facilitare la collaborazione tra le Autorità nazionali di notifica e di supervisione del mercato. Le responsabilità del Consiglio comprendono il coordinamento nell'applicazione

del Regolamento, offrendo consulenza e potendo produrre raccomandazioni e pareri scritti. Tra i suoi compiti specifici, il Consiglio supporta le Autorità nazionali e la Commissione nello sviluppo delle capacità necessarie per implementare il Regolamento, esprime valutazioni sulle segnalazioni qualificate riguardanti i modelli di IA per finalità generali e raccoglie i pareri degli Stati membri.

Il Forum consultivo, svolge un ruolo consultivo e di supporto tecnico per il Consiglio e la Commissione. È formato da rappresentanti dell'industria, delle startup, delle piccole e medie imprese, della società civile e del mondo accademico, nominati dalla Commissione per un mandato di 2 anni, estendibile a quattro. Gli enti di standardizzazione europei CEN, CENELEC ed ETSI hanno una rappresentanza permanente all'interno del Forum Consultivo come membri di diritto.

Il Gruppo di esperti scientifici indipendenti, con competenze tecniche nel campo dell'IA che deve fornire consulenza e supporto all'Ufficio dell'AI per l'implementazione del Regolamento ed eventuale sostegno alle Autorità nazionali di vigilanza del mercato. Gli Stati membri possono richiedere l'intervento del Gruppo, previo pagamento di compensi che verranno definiti in atti di esecuzione della Commissione.

7.2. Autorità nazionali competenti

L'AI Act prevede anche la competenza delle Autorità nazionali per l'applicazione e la supervisione delle norme nei rispettivi Stati membri. Esse operano in sinergia con le istituzioni europee, garantendo un controllo decentralizzato, ma coordinato a livello dell'Unione.

A livello nazionale, ciascuno Stato membro deve identificare una o più Autorità competenti per l'applicazione del Regolamento, tra cui almeno un'Autorità di notifica (che deve gestire l'accreditamento degli organismi indipendenti che svolgono le valutazioni di conformità esterne) e almeno un'Autorità di sorveglianza del mercato (con compiti di vigilanza e sanzionatori). Ad una terza autorità, o organismo pubblico, deve essere affidato il compito di sorvegliare o far rispettare gli obblighi dell'Unione a tutela dei diritti fondamentali, compreso il diritto alla non discriminazione, in relazione all'uso dei sistemi di IA ad alto rischio.

Le tre Autorità così designate hanno compiti differenti tra loro:

- l'**Autorità di notifica** opera prima dell'immissione sul mercato del sistema di IA, verificando che il processo di conformità per la commercializzazione sia stato seguito correttamente;
- l'**Autorità di sorveglianza del mercato** interviene dopo la commercializzazione del sistema di IA, controllando il mantenimento dei requisiti regolamentari. Ha poteri investigativi e sanzionatori, può classificare i sistemi nelle categorie previste dal Regolamento e intervenire anche su sistemi formalmente conformi, ma potenzialmente rischiosi per salute, sicurezza, diritti fondamentali o sicurezza pubblica;
- l'**Autorità di tutela dei diritti fondamentali** può sollecitare l'intervento dell'Autorità di sorveglianza del mercato quando sospetta che si verifichino violazioni degli obblighi europei sui diritti fondamentali.

8. Sanzioni (art. 99-101, cons. 168-169)

L'AI Act stabilisce delle soglie di sanzioni fino al limite massimo, in particolare:

- **fino a 35 milioni di euro o al 7% del fatturato totale annuo a livello mondiale** dell'esercizio finanziario precedente (a seconda di quale sia il valore più alto) per le violazioni relative alle pratiche vietate;
- **fino a 15 milioni di euro o al 3% del fatturato totale annuo a livello mondiale** dell'esercizio finanziario precedente per la mancata osservanza di uno qualsiasi degli altri requisiti o obblighi del Regolamento, compresa la violazione delle norme sui modelli di IA per uso generale;
- **7,5 milioni di euro o all'1,5% del fatturato mondiale annuo totale** dell'esercizio precedente per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle Autorità nazionali.

In sostanza le sanzioni pecuniarie si differenziano a seconda del **tipo di sistema di IA** e anche **in relazione ai soggetti** che hanno posto in essere la violazione**, per chiarezza uno schema di sintesi:**

Violazione	Sanzione
Sistemi di IA vietati	Sanzione fino a € **35.000.000** o **7%** del fatturato mondiale annuale riferito all'anno precedente, se superiore
Violazioni attuate dai seguenti soggetti e relativi ad obblighi specifici: • **Obblighi dei fornitori** • **Obblighi dei rappresentanti autorizzati** • **Obblighi degli importatori** • **Obblighi dei distributori** • **Obblighi dei deployer**	Sanzione fino a € **15.000.000** o **3%** del fatturato mondiale annuale riferito all'anno precedente, se superiore

• **Obblighi degli organismi notificati** • **Obblighi di trasparenza per i fornitori e gli utilizzatori**	
Trasmissione di informazioni non corrette, incomplete o fuorvianti agli organismi notificati	Sanzione fino a € **7.500.000** o **1%** del fatturato mondiale annuale riferito all'anno precedente, se superiore
Modelli di IA per finalità generali (sanzioni applicate dalla Commissione europea): • **Violazione delle disposizioni del Regolamento** • **Inottemperanza a una richiesta di informazioni o resa di informazioni inesatte, incomplete o fuorvianti;** • **Non ottemperanza a una misura richiesta dalla Commissione** • **Mancata messa a disposizione dell'accesso al modello al fine della valutazione della Commissione.**	Sanzione fino a € **15.000.000** o **3%** del fatturato mondiale annuale riferito all'anno precedente, se superiore

Tabella 6. Quadro delle saznioni.

9. Tempi per l'applicazione e revisione del Regolamento

9.1. Entrata in vigore e periodo di transizione

L'art. 113 stabilisce che il Regolamento entrerà in vigore il 2 agosto 2024 e **si applicherà dal 2 agosto 2026**.

La stessa norma prevede tuttavia delle **deroghe** suddivise in tre gruppi:

- **Norme che saranno applicate dal 2 febbraio 2025**: disposizioni generali (capo I) e in particolare l'art. 4 su "alfabetizzazione in materia di IA", e le pratiche vietate (art. 5)
- **Norme che saranno applicate dal 2 agosto 2025**: disposizioni che riguardano le Autorità designate dagli Stati membri (Capo III, Sez. 4), la disciplina della trasparenza dei sistemi di IA, la regolamentazione dei modelli IA per finalità generali (capo V), le sanzioni a eccezione dell'art. 101 (capo XII) e la disciplina sulla riservatezza delle informazioni rese alle Autorità (art. 78);
- **Norme che saranno applicate dal 2 agosto 2027:** ossia le disposizioni relative ai sistemi ad alto rischio di cui in Allegato I.

9.2. Termini di adeguamento per i sistemi di IA immessi sul mercato (art. 111)

Fatta salva l'applicazione dell'art. 5 sulle pratiche vietate a decorrere dal 2 febbraio 2025, l'AI Act stabilisce (art. 111, par. 1) che i sistemi di IA componenti dei sistemi IT su larga scala relativi al sistema di informazione Schengen, al sistema di informazione visti, Eurodac, al sistema di ingressi/uscite, al sistema europeo di informazione e autorizzazione ai viaggi, al sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di paesi terzi e apolidi, all'interoperabilità su frontiere, visti e cooperazione di polizia e giudiziaria istituiti con gli atti normativi indicati nell'Allegato X del Regolamento, e che sono stati immessi sul mercato o messi in servizio prima del 2 agosto 2027, dovranno adattarsi all'AI Act entro il **31 dicembre 2030**.

Invece, per i sistemi IA **ad alto rischio diversi da quelli sopra descritti, immessi sul mercato prima del 2 agosto 2026,** si applicherà l'AI Act solo se a partire da tale data i sistemi saranno oggetto di modifiche significative della loro progettazione.

In ogni caso i fornitori e deployers di sistemi di IA ad alto rischio che sono destinati ad essere utilizzati dalle **autorità pubbliche, dovranno conformarsi entro il 2 agosto 2030**.

Infine, i fornitori di **modelli di IA per finalità generali** immessi sul mercato **prima** del **2 agosto 2025** dovranno conformarsi agli obblighi del regolamento entro il **2 agosto 2027**.

9.3. Valutazione dello stato di adeguamento e revisione del Regolamento (art. 112)

Considerando l'evoluzione continua del fenomeno dell'intelligenza artificiale, lo stesso Regolamento prevede la possibilità di valutazioni inerenti lo stato di applicazione dell'AI Act e l'adeguatezza della normativa rispetto agli sviluppi, al fine di individuare eventuali carenze della stessa.

Pertanto, la Commissione è chiamata a presentare tali valutazioni almeno fino alla scadenza della delega di potere riconosciuta, ex art. 97, dal **1° agosto 2024 e per i successivi cinque anni**.

La Commissione, inoltre, è tenuta annualmente a valutare se sia opportuno aggiornare l'Allegato III (relativo all'individuazione delle casisistiche in cui il sistema è considerato ad alto rischio).

Entro il 2 agosto 2028 la Commissione deve valutare e poi riferire al Consiglio per l'IA europeo, eventuali modifiche da apportare a diversi punti del Regolamento (fra cui misure di trasparenza e sistema di *governance*, sviluppo dei prodotti sotto il profilo energetico dei modelli GPAI).

Poi sempre **entro il 2 agosto 2028 e successivamente, ogni tre anni**, la Commissione deve valutare l'efficacia dei codici di condotta volontari.

Per quanto riguarda, invece, la valutazione circa lo stato di applicazione del Regolamento che la Commissione deve presentare al Parlamento e al Consiglio, **il termine è il 2 agosto 2029 e poi ogni quattro anni.**

Ultimo termine previsto è il 2 agosto 2031 per una valutazione da presentare al Parlamento, al Consiglio e al Comitato economico e sociale europeo, in merito all'esecuzione del Regolamento e ad eventuali necessarie modifiche.

ALLEGATO: IL PERCORSO DELL'AI ACT

L'Unione Europea per l'adozione del Regolamento (UE) 2024/1689 (di seguito anche "Regolamento" o "AI Act) ha seguito un percorso strutturato, partito da alcune considerazioni del Parlamento Europeo sulla robotica per poi fissare alcuni principi ed orientamenti etici volti a fornire la base per le successive regole giuridiche.

Sono di matrice europea i principi di "human-centric AI" (nel rispetto dei diritti fondamentali dell'Unione) e di "trustworthy AI", ossia di sistemi di intelligenza artificiale affidabile (dal punto di vista tecnologico, etico e giuridico) che fortemente impregnano il Regolamento.

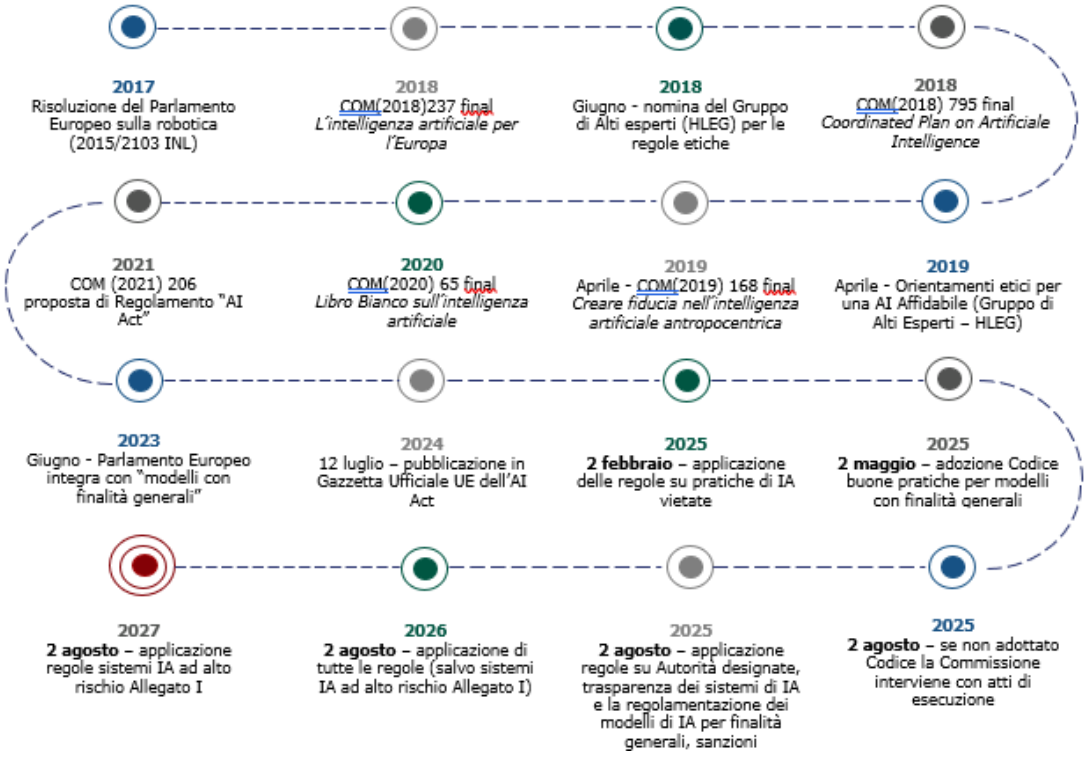

Figura 1. Il "Percorso" dell'AI Act.

LE REGOLE ETICHE

Nell'aprile del 2019 il Gruppo di esperti di alto livello sull'intelligenza artificiale pubblicava il documento Orientamenti etici per un'IA affidabile.

In più parti gli Orientamenti richiamano i diritti fondamentali dell'uomo, contenuti nella CEDU e nel Trattato UE che vengono posti come base di partenza dei principi etici.

Gli Orientamenti fissano innanzitutto alcuni principi e valori generali affinché un sistema di intelligenza artificiale possa essere considerato un sistema "antropocentrico" (human-centered) e ritenuto affidabile (trustworthy AI). Per poter avere tali caratteristiche il sistema deve possedere tre componenti:

- la **legalità**, nel senso che deve ottemperare a tutte le leggi e a tutti i regolamenti applicabili;
- **l'eticità**, assicurando l'adesione a principi e valori etici;
- la **robustezza**, da un punto di vista tecnico e sociale.

Tali componenti, pur se necessarie per l'IA affidabile, non sono sufficienti, dato che gli Orientamenti stabiliscono che il sistema deve anche soddisfare i seguenti principi:

- il principio della **prevenzione dei danni**, inteso sia come principio di beneficenza (fai il bene) sia come principio di non maleficenza (non fare il male);
- il principio del **rispetto dell'autonomia umana** (preservare l'agente umano): che richiede il rispetto del principio di auto-determinazione dell'uomo;
- il **principio di equità** (sii equo): nel contesto dell'intelligenza artificiale affidabile è necessario evitare discriminazioni o pregiudizi, eliminando bias ed errori, al fine di assicurare il pari trattamento degli esseri umani;
- il **principio di esplicabilità** (opera in maniera trasparente): ossia la possibilità di controllare il sistema decisionale di un'intelligenza artificiale, che dovrebbe essere comprensibile per gli uomini.

Gli Orientamenti contengono una serie di requisiti specifici e concreti, in alcuni casi vere e proprie indicazioni di implementazione, affinché un sistema di IA sia "etico by design". Sono requisiti specifici che comprendono aspetti sistemici, individuali e sociali:

- intervento e sorveglianza umani (inclusi i diritti fondamentali, l'intervento umano e la sorveglianza umana);

- robustezza tecnica e sicurezza (inclusi la resilienza agli attacchi e la sicurezza, piani di emergenza e la sicurezza generale, la precisione, l'affidabilità e la riproducibilità);
- riservatezza e governance dei dati (inclusi il rispetto della riservatezza, la qualità e l'integrità dei dati e l'accesso ai dati);
- trasparenza (incluse la tracciabilità, la spiegabilità e la comunicazione);
- diversità, non discriminazione ed equità (incluse la prevenzione di distorsioni inique, l'accessibilità e la progettazione universale, la partecipazione dei portatori di interessi);
- benessere sociale e ambientale (inclusi la sostenibilità e il rispetto ambientale, l'impatto sociale, la società e la democrazia);
- accountability (inclusi la verificabilità, la riduzione al minimo degli effetti negativi e la loro segnalazione, i meccanismi di ricorso verso le decisioni dei sistemi di IA).

La terza parte delle linee guida termina con l'indicazione di metodi tecnici e non tecnici per realizzare un'IA affidabile, introducendo anche una sorta di checklist per svolgere una valutazione circa il grado di "eticità" del sistema.

DALL'ETICA AL DIRITTO: LE SCELTE DELLA COMMISSIONE EUROPEA

Gli Orientamenti etici hanno fortemente improntato le scelte della Commissione Europea, intenzionata a creare un ecosistema di eccellenza inteso quali misure per sostenere la ricerca, la collaborazione tra gli Stati membri e gli investimenti nello sviluppo e diffusione dell'IA, sostenuto da un ecosistema della fiducia, con al centro il rispetto dei diritti fondamentali dell'UE.

Per realizzare tale ecosistema di fiducia nella nuova tecnologia dell'intelligenza artificiale la Commissione si è orientata per introdurre un pacchetto completo di misure per affrontare i problemi posti dall'introduzione e dall'utilizzo dell'IA, adottando tre iniziative correlate:

- un quadro giuridico europeo per l'IA per tutelare i diritti fondamentali e i rischi per la sicurezza specifici dei sistemi di IA (l'AI Act);

- norme UE per affrontare le questioni di responsabilità legate alle nuove tecnologie, compresi i sistemi di IA (non oggetto dell'AI Act ma di separati atti normativi);
- revisione della legislazione settoriale sulla sicurezza dei prodotti.

La valutazione di impatto del Regolamento svolge alcune considerazioni anche relativamente al contesto socioeconomico dell'Unione Europea, concentrandosi sulle opportunità ed i rischi che potrebbero derivare dalla diffusione dei sistemi di intelligenza artificiale. Se da una parte questi potrebbero portare progressi in molti settori, dalle diagnosi mediche alla lotta ai cambiamenti climatici, contribuendo a risolvere problemi complessi per il bene pubblico ed al raggiungimento degli obiettivi di sviluppo sostenibile delle Nazioni Unite, con un impatto economico di migliaia di miliardi di euro sull'economia globale entro il 2030, viene sottolineato come l'Europa sia in una posizione arretrata rispetto ad altre zone geografiche del mondo, ospitando solo 3 dei 25 principali cluster di IA a livello mondiale ed avendo solo un terzo del numero di aziende nel settore di questa tecnologia per milione di dipendenti rispetto gli Stati Uniti.

Il nuovo Regolamento, inoltre, si innesta su un quadro giuridico già volto a tutelare una serie di posizioni giuridiche dei cittadini dell'Unione, in particolare:

- i diritti fondamentali, considerati dalla Carta dei diritti fondamentali dell'UE quelli della dignità umana, la libertà, l'uguaglianza, la solidarietà, la cittadinanza e la giustizia, che devono essere rispettati nello sviluppo e nell'uso dell'IA;
- il Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali;
- le direttive UE esistenti in materia di parità che proibiscono la discriminazione basata su una serie di motivi (come l'origine razziale ed etnica, la religione, il sesso, l'età, la disabilità e l'orientamento sessuale) ed in contesti e settori specifici (ad esempio, occupazione, istruzione, protezione sociale, accesso a beni e servizi);
- la normativa a tutela dei consumatori, con il divieto di pratiche commerciali sleali;

- la legislazione pertinente in materia di sicurezza dei prodotti[2].
- responsabilità: le direttive sulla responsabilità per danno da prodotti difettosi e sul credito al consumo allocano le responsabilità tra produttori e utenti. Tuttavia, caratteristiche dell'IA come opacità, autonomia, dipendenza dai dati creano incertezza nell'applicazione di queste norme.

In considerazione di tale contesto normativo la Commissione ha adottato un approccio graduale per la regolamentazione dell'intelligenza artificiale, affrontando prima il profilo della regolamentazione dei sistemi IA come prodotti per poi definire meglio le regole di imputazione della responsabilità civile.

Il Regolamento intende risolvere principalmente sei problemi essenziali che sono dettagliatamente elencati ed esaminati nella valutazione di impatto predisposta dalla Commissione:

[2] Nel contesto della legislazione UE sulla sicurezza specifica dei prodotti, si distinguono tradizionalmente i cosiddetti «vecchi approcci» e «nuovi approcci». Il «vecchio approccio» si riferisce alla fase iniziale della regolamentazione UE sui prodotti, la cui caratteristica principale era l'inclusione di requisiti tecnici dettagliati nel corpo della legislazione. Alcuni settori, come quello alimentare o dei trasporti, sono ancora regolamentati sulla base di legislazioni del «vecchio approccio» con requisiti di prodotto dettagliati per ragioni di politiche pubbliche o per la loro dipendenza da tradizioni e/o accordi internazionali che non possono essere modificati unilateralmente. Nel 1985 è stato sviluppato il cosiddetto «nuovo approccio», il cui obiettivo principale era quello di limitare il contenuto della legislazione ai «requisiti essenziali (di alto livello)», lasciando i dettagli tecnici alle norme armonizzate europee. Sulla base del Nuovo Approccio, nel 2008 è stato sviluppato il NLF (New Legal Framework) definito dal Regolamento 765/2008 che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti, dalla Decisione 768/2008/EC relativa a un quadro comune per la commercializzazione dei prodotti e dal Regolamento 764/2008 che stabilisce procedure relative all'applicazione di determinate norme tecniche nazionali a prodotti legalmente commercializzati in un altro Stato membro.

PROBLEMI PRINCIPALI	PARTI INTERESSATE
1. L'uso dell'IA comporta maggiori rischi per la sicurezza e l'incolumità dei cittadini.	Cittadini, consumatori e altre vittime Imprese interessate
2. L'uso dell'IA comporta un maggior rischio di violazione dei diritti fondamentali dei cittadini e dei valori dell'Unione.	Cittadini, consumatori e altre vittime. Interi gruppi
3. Le autorità non hanno poteri, framework procedurali e le risorse per garantire e monitorare la conformità dello sviluppo e dell'utilizzo dell'IA alle norme applicabili	Autorità nazionali responsabili del rispetto delle norme di sicurezza e dei diritti fondamentali
4. L'incertezza e la complessità giuridica sulle modalità di applicazione delle norme esistenti ai sistemi di IA dissuadono le imprese dallo sviluppare e utilizzare i sistemi di IA.	Imprese e altri fornitori che sviluppano sistemi di intelligenza artificiale Aziende e altri utenti che utilizzano sistemi di intelligenza artificiale
5. La sfiducia nell'IA rallenterebbe lo sviluppo dell'IA in Europa e ridurrebbe la competitività globale dell'economia dell'UE.	Imprese e altri utenti che utilizzano sistemi di IA Cittadini che utilizzano sistemi di IA o che ne sono influenzati
6. Misure frammentate creano ostacoli al mercato unico dell'IA e minacciano la sovranità digitale dell'Unione.	Imprese che sviluppano l'IA, soprattutto PMI interessate Utenti del sistema di IA, compresi i consumatori, Imprese e autorità pubbliche

Tabella 7. Valutazione di impatto dell'AI Act – Commissione Europea

Gli obiettivi del Regolamento, pertanto, sono molteplici in quanto coinvolgono sia tematiche inerenti alla protezione dei diritti, sia la necessità di evitare una frammentazione normativa tra i vari Stati membri, che potrebbe andare a scapito del mercato comune, oltre alla necessità di creare un sostrato di fiducia per l'utilizzo dei sistemi di IA, favorendone così lo sviluppo e la diffusione nella UE e, infine, definire i poteri di vigilanza delle Autorità di controllo.

In tale quadro la Commissione ha esaminato 4 approcci regolatori (anzi 4+1), ossia:

- uno schema di etichettatura volontario (opzione 1): che consente ai fornitori di certificare la conformità dei sistemi di IA a determinati requisiti per un'IA affidabile, ottenendo così una «etichetta UE»;
- l'approccio settoriale ad hoc (opzione 2): ossia disposizioni specifiche per singoli settori, con regole volte a disciplinare i casi d'uso per settore;
- una norma di portata orizzontale con approccio risk based (opzione 3), con un'unica definizione di IA e requisiti ed obblighi orizzontali armonizzati;

- una norma di portata orizzontale con approccio risk based e codici di condotta settoriali per IA non ad alto rischio (opzione 3+), sostanzialmente analoga all'opzione 3, ma con la possibilità di prevedere dei Codici di condotta volontari;
- una norma di portata orizzontale analoga per tutti i sistemi IA, ossia senza graduazione di obblighi, ma applicazione uniforme della disciplina a tutti i fornitori.

Tra i vari elementi presi in considerazione dalla Commissione ai fini della decisione su quale opzione di politica legislativa adottare in materia di intelligenza artificiale, vi è anche quello dei costi che ciascun approccio avrebbe comportato per le imprese e gli utilizzatori. L'analisi è stata condotta considerando costi aggregati di conformità e amministrativi per l'adeguamento dei sistemi di IA alle previsioni normative, nonché costi di verifica ex post.

	CONFORMITÀ + COSTI AMMINISTRATIVI	COSTI DI VERIFICA
Opzione 1	Tra 0 e 3 miliardi di euro (tutti volontari)	**€ 0**
Opzione 2	n/a	**n/a**
Opzione 3	Tra 100 e 500 milioni di euro	**Circa 100 milioni di euro**
Opzione 3+	Tra 100/500 milioni di euro e 3 miliardi di euro (volontario sopra 100/500 milioni di euro)	**Poco più di 100 milioni di euro**
Opzione 4	**Circa 3 miliardi di euro nel 2025**	**Tra 1 e 3 miliardi di euro**

Tabella 8. Tabella dei costi aggregati dalla valutazione di impatto Commissione Europea

Secondo la Commissione Europea dal punto di vista dell'impatto sulle PMI l'opzione 1 (sistema di etichettatura volontaria) garantirebbe la proporzionalità, mentre l'opzione 2 (regolamentazione ad hoc) potrebbe aumentare gli oneri amministrativi per le PMI che lavorano su diverse applicazioni.

Le opzioni 3 e 3+ (requisiti per le applicazioni ad alto rischio) manterrebbero i costi al minimo e garantirebbero la proporzionalità, con benefici come una maggiore certezza giuridica e l'accesso al mercato unico, coinvolgendo anche PMI minori. Queste, nel caso di produzione di sistemi ad alto rischio, sarebbero più colpite rispetto alle grandi aziende a causa di economie di scala e di scopo limitate e di una minore capacità finanziaria, ma beneficerebbero

maggiormente di un aumento della fiducia nell'IA. Le sandbox normative e gli standard armonizzati faciliterebbero la conformità per le PMI.

L'opzione 4 (requisiti orizzontali per tutte le applicazioni di IA) esporrebbe le PMI a costi sproporzionati.

Sulla base del confronto tra i costi e i benefici, non solo economici, delle varie opzioni, la Commissione ha ritenuto preferibile l'opzione 3+ relativa a un quadro normativo per le applicazioni di IA ad alto rischio con la possibilità, per quelle non ad alto rischio, di seguire dei codici di condotta, scelta poi tradotta nella proposta di Regolamento.

È interessante notare che la valutazione di impatto, nello stimare i costi derivanti dalla scelta normativa, non poteva tener conto delle modifiche che sono state inserite dal Parlamento Europeo a giugno 2023 nella proposta regolamentare, in particolare introducendo nuove disposizioni al fine di regolare anche l'immissione e uso sul mercato europeo dei modelli di IA per finalità generali con disposizioni che estendono i requisiti di conformità e gli oneri amministrativi e di controllo ex post anche a tali modelli, così introducendo ulteriori costi originariamente non oggetto di valutazione.