AI ACT in pratica: dalla normativa all'implementazione, con il supporto dell' AI generativa

Giancarlo Butti



Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80.
Referente Regolamento DORA e Inclusion del Comitato Scientifico del CLUSIT.
Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni.
Oltre 200 corsi e seminari tenuti presso ISACA, ORACLE, CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CA FOSCARI, UNIVERSITA' SUOR ORSOLA BENINCASA NAPOLI, UNIVERSITA' DEL MOLISE, CEFRIEL, AIIA, ABI e master presso diversi atenei; già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer.
Ha all'attivo oltre 900 articoli e collaborazioni con oltre 40 testate.
Ha pubblicato 32 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 35 opere collettive nell'ambito di ABI LAB, Oracle-CLUSIT Community for Security, Rapporto CLUSIT.
Socio e già proboviro di ISACA/AIEA è socio del CLUSIT, di ACFE, di DFA, di AIPIA e del BCI e partecipa a numerosi gruppi di lavoro.
Ha inoltre acquisito le certificazioni/qualificazioni (LA BS 7799), (LA ISO IEC 27001:2005/2013/2022), (LA ISO 20000-1), (LA ISO 22301), (LA ISO IEC 42001), CRISC, CDPSE, ISM, DPO, DPO UNI 11697:2017, DPO UNI CEI EN 17740:2024, CBCI, AMBCI.

Note sul copyright

IN PREPARAZIONE





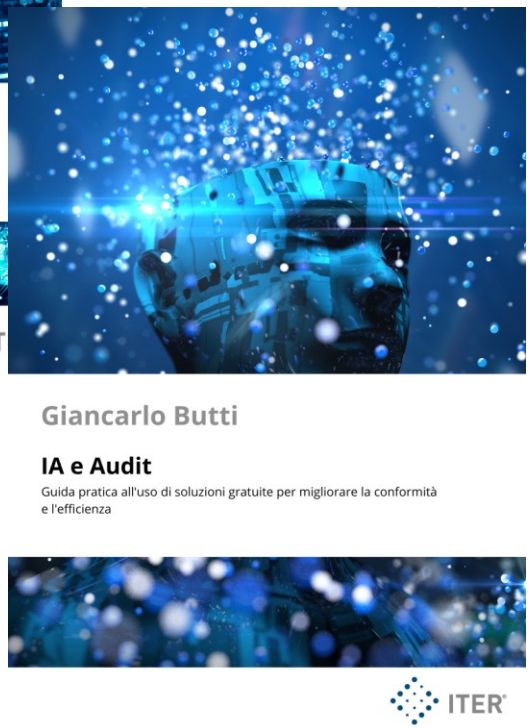
Alcuni testi e applicazioni derivano da queste mie pubblicazioni

Note sul copyright

Alcuni testi e applicazioni derivano da queste mie pubblica







https://iterdigital.it/it_it/ia-e-audit/#1759849267092-0aa1d321-1fd7
https://iterdigital.it/it_it/gestione-rischi-supply-chain/#1759849542919-e116777c-a7f0
https://iterdigital.it/it_it/download/22185/

Gli altri miei libri sull'AI



AI Act



AI Act
Regolamento 2026/1744

AI Act

- Oggetto, definizione e ambito di applicazione
- Classificazione dei sistemi di IA e pratiche di IA vietate
- Obblighi di trasparenza per determinati sistemi di IA e modelli di IA per finalità generali
- Eccezioni previste per le autorità di contrasto
- Sistemi di IA per finalità generali e modelli fondativi o di base
- Misure a sostegno dell'innovazione
- Architettura di governance
- Sistemi di IA già immessi sul mercato o messi in servizio
- Sanzioni
- Misure di attuazione
- Entrata in vigore

Architettura della normativa

Il Regolamento è composto da:

- 180 considerando
- 113 articoli
- 13 allegati

Architettura della normativa

Dei 113 articoli circa 40 sono prescrittivi per i soggetti che operano con sistemi AI **e quindi hanno interesse per le attività di audit.**

La normativa è molto squilibrata, in quanto:

- la quasi totalità delle prescrizioni (circa 30 articoli) riguarda i sistemi ad alto rischio
  - quasi tutte le prescrizioni sono rivolte ai fornitori di sistemi
  - gli utilizzatori di sistemi di AI hanno un numero limitato di prescrizioni
- alcune prescrizioni riguardano modelli di IA per finalità generali
- na prescrizione riguarda gli obblighi di trasparenza per i fornitori e i deployer di determinati sistemi di IA
- le prescrizioni di carattere generale sono limitate.

Commission Guidelines on the definition of an artificial intelligence system established by Regulation EU 2024/1689 – AI Act

Only certain AI systems are subject to regulatory obligations and oversight under the AI Act. The AI Act's risk-based approach means that only those systems giving rise to the most significant risks to fundamental rights and freedoms will be subject to its prohibitions laid down in **Article 5 AI Act**, its regulatory regime for high-risk AI systems covered by **Article 6 AI Act** and its transparency requirements for a limited number of pre-defined AI systems laid down in **Article 50 AI Act**. **The vast majority of systems, even if they qualify as AI systems within the meaning of Article 3(1) AI Act, will not be subject to any regulatory requirements under the AI Act.**

Fornitori di sistemi AI

«fornitore»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito;

Articolo 25 - ***Responsabilità lungo la catena del valore dell'IA***

1.Qualsiasi distributore, importatore, deployer o altro terzo è considerato fornitore di un sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetto agli obblighi del fornitore a norma dell'articolo 16, nelle circostanze seguenti:

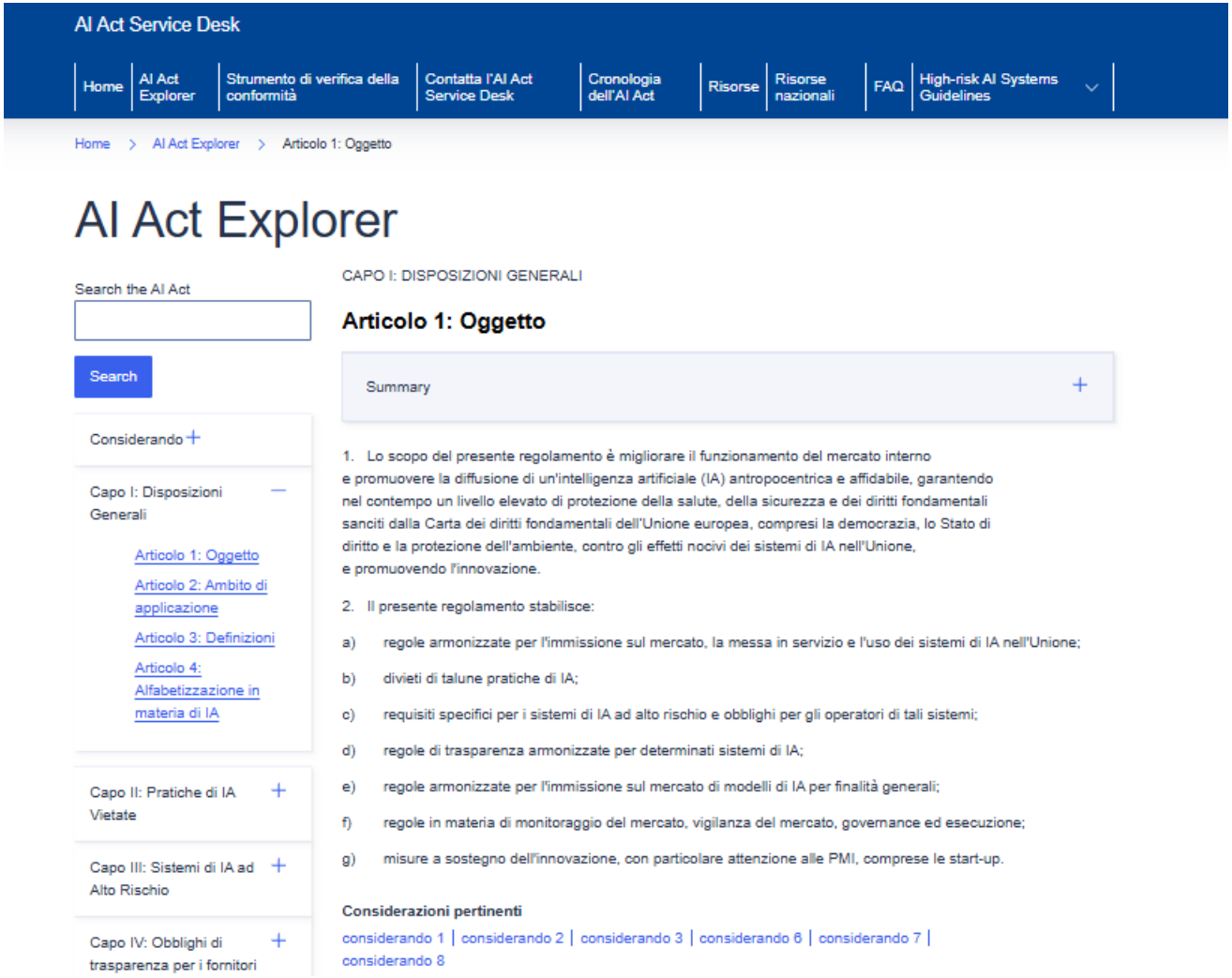
- *se appone il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi al riguardo;*
- *se apporta una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o già messo in servizio in modo tale che resti un sistema di IA ad alto rischio a norma dell'articolo 6;*
- *se modifica la finalità prevista di un sistema di IA, anche un sistema per finalità generali, che non è stato classificato come ad alto rischio e che è già stato immesso sul mercato o messo in servizio in modo tale che il sistema di IA interessato diventi un sistema di IA ad alto rischio a norma dell'articolo 6.*

Sommario

- Capo I: Disposizioni Generali
- Capo II: Pratiche di IA Vietate
- Capo III: Sistemi di IA ad Alto Rischio
- Capo IV: Obblighi di trasparenza per i fornitori e i deployers di determinati sistemi di IA
- Capo V: Modelli di IA per finalitá generali
- Capo VI: Misure a sostegno dell'innovazione
- Capo VII: Governance
- Capo VIII: Banca dati dell'UE per i sistemi di IA ad alto rischio
- Capo IX: Monitoraggio successivo all'immissione sul mercato, condivisione delle informazioni e vigilanza del mercato
- Capo X: Codici di condotta e orientamenti
- Capo XI: Delega di potere e procedura di comitato
- Capo XII: Sanzioni
- Capo XIII: Disposizioni finali

Sommario

- ALLEGATO I - Elenco della normativa di armonizzazione dell'Unione
- ALLEGATO II - Elenco dei reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii)
- ALLEGATO III - Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2
- ALLEGATO IV - Documentazione tecnica di cui all'articolo 11, paragrafo 1
- ALLEGATO V - Dichiarazione di conformità UE
- ALLEGATO VI - Procedura di valutazione della conformità basata sul controllo interno
- ALLEGATO VII - Conformità basata su una valutazione del sistema di gestione della qualità e su una valutazione della documentazione tecnica
- ALLEGATO VIII - Informazioni da presentare all'atto della registrazione di sistemi di IA ad alto rischio in conformità dell'articolo 49
- ALLEGATO IX - Informazioni da presentare all'atto della registrazione dei sistemi di IA ad alto rischio elencati nell'allegato III in relazione alle prove in condizioni reali in conformità dell'articolo 60
- ALLEGATO X - Atti legislativi dell'Unione sui sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia
- ALLEGATO XI - Documentazione tecnica di cui all'articolo 53, paragrafo 1, lettera a) — documentazione tecnica per i fornitori di modelli di IA per finalità generali
- ALLEGATO XII - Informazioni sulla trasparenza di cui all'articolo 53, paragrafo 1, lettera b) - documentazione tecnica per i fornitori di modelli di IA per finalità generali ai fornitori a valle che integrano il modello nel loro sistema di IA
- ALLEGATO XIII - Criteri per la designazione dei modelli di IA per finalità generali con rischio sistemico di cui all'articolo 51



https://ai-act-service-desk.ec.europa.eu/it/ai-act/article-1

Oggetto, definizione e ambito di applicazione

Il regolamento ha l'obiettivo di migliorare il funzionamento del mercato interno e promuovere l'adozione di un'intelligenza artificiale affidabile e incentrata sull'uomo, garantendo, nel contempo, un elevato livello di **protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dell'UE**, compresa la democrazia, lo Stato di diritto e la tutela dell'ambiente dagli effetti dannosi dei sistemi di intelligenza artificiale nell'Unione, nonché sostenendo l'innovazione.

Definizione – sistema AI

La definizione di sistema di IA formulata nel regolamento è quella di

«sistema di IA»: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

Alla Commissione europea è demandata l'adozione di linee guida sull'applicazione della richiamata definizione di sistema di IA.

La definizione originariamente proposta dalla Commissione è stata modificata nel corso del negoziato allo scopo di allinearla all'approccio dell'OCSE.

Definizioni – Modello AI

«modello di IA per finalità generali»: un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato;

Sistemi e modelli AI

La legge sull'IA distingue tra un sistema di IA, definito all'articolo 3, paragrafo 1, e un modello di IA per finalità generali, definito all'articolo 3, paragrafo 63.

La legge sull'IA fa riferimento ai modelli di IA come a quelli che "sono componenti essenziali dei sistemi di IA. Non costituiscono sistemi di IA da soli. I modelli di IA richiedono l'aggiunta di ulteriori componenti, come ad esempio un'interfaccia utente, per diventare sistemi di IA. I modelli di IA sono generalmente integrati nei sistemi di IA e ne fanno parte" (considerando 97). "I modelli di IA generativa di grandi dimensioni sono un tipico esempio di modello di IA per finalità generali, dato che consentono una generazione flessibile di contenuti, ad esempio sotto forma di testo, audio, immagini o video, che possono facilmente ospitare un'ampia gamma di compiti distintivi" (considerando 99).

La legge sull'IA definisce un sistema di IA come un "sistema basato su macchine progettato per funzionare con diversi livelli di autonomia e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce, dall'input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare gli ambienti fisici o virtuali" (articolo 3, paragrafo 1, considerando 1

Composizione

Il nuovo regolamento introduce:

a) regole armonizzate per **l'immissione sul mercato, la messa in servizio e l'uso** dei sistemi di intelligenza artificiale nell'Unione;

b) il **divieto** di determinate pratiche di intelligenza artificiale;

c) **requisiti specifici per i sistemi di IA ad alto rischio** e obblighi per gli operatori di tali sistemi;

d) regole di **trasparenza** armonizzate per alcuni sistemi di IA;

e) **regole** armonizzate specifiche per l'immissione sul mercato di **modelli di IA di uso generale**;

f) **regole sul monitoraggio del mercato, sulla governance e sull'applicazione della vigilanza del mercato stesso**;

g) misure a **sostegno dell'innovazione**, con particolare attenzione alle PMI, comprese le start-up.

Applicabilità

Il regolamento si **applicherà ai soggetti pubblici e privati**, all'interno e all'esterno dell'UE, a condizione che il sistema di IA sia **immesso sul mercato dell'Unione** o che il **suo uso abbia effetti su persone situate nell'UE.**

Riguarderà sia i **fornitori** (ad es. uno sviluppatore di uno strumento di screening dei CV) che gli **operatori** (*deployer*) di sistemi di IA ad alto rischio (ad es. una banca che acquista uno strumento di screening dei CV).

Gli **importatori** di sistemi di IA dovranno inoltre garantire che il fornitore straniero abbia già eseguito l'appropriata procedura di **valutazione della conformità**, che il sistema rechi una **marcatura di conformità europea (CE)** e sia **corredato della documentazione e delle istruzioni per l'uso richieste.**

AI Act: una normativa per tutti, ma con impatti rilevanti solo per pochi

Adottare l'AI Act: gli errori da evitare e la gap analysis da fare

ADEMPIMENTI

La classificazione nell'AI ACT: i 4 livelli di rischio

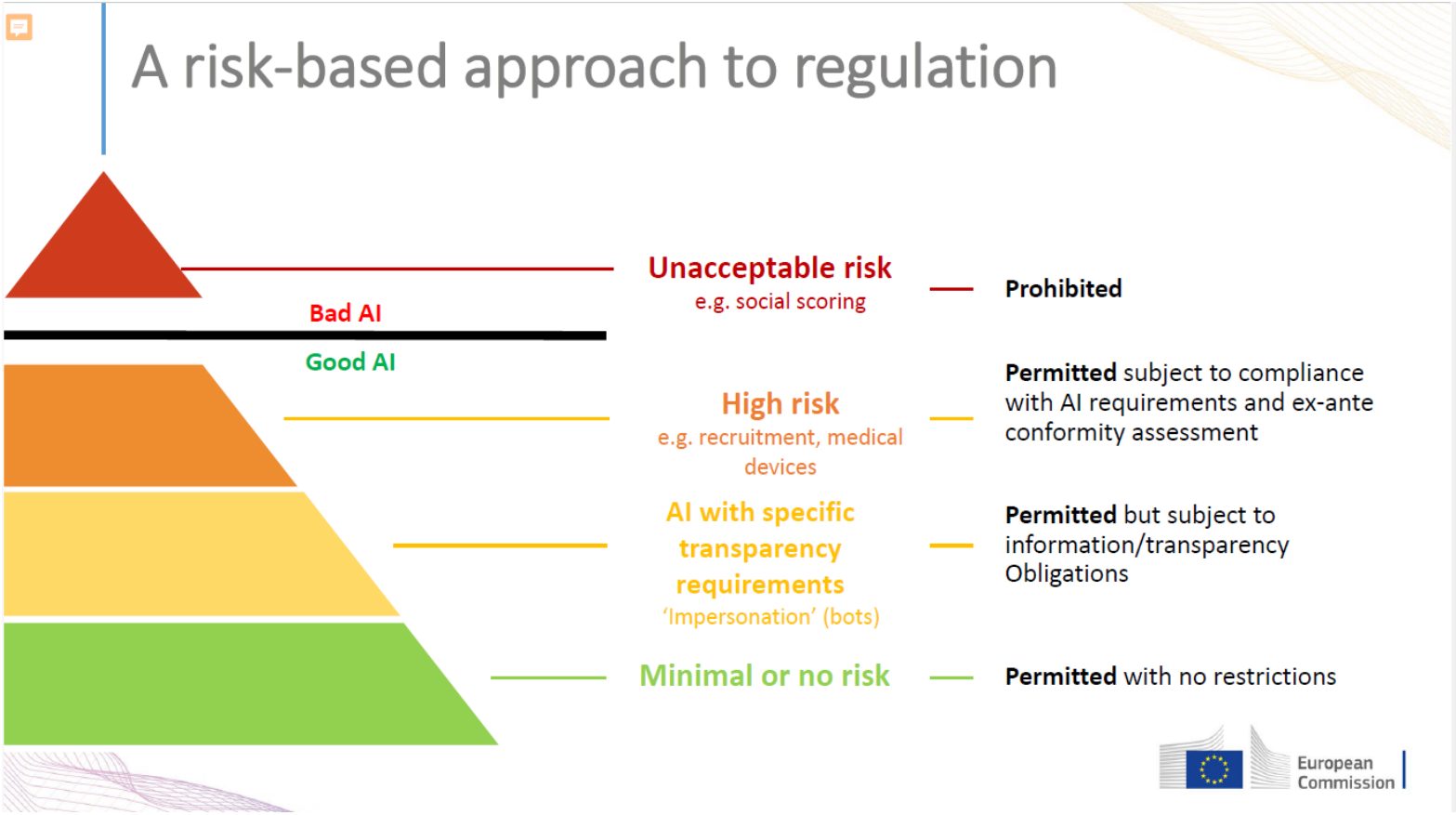
LA GUIDA

AI Act, sistemi ad alto rischio: come ridurre drasticamente oneri e rischi

I sistemi che l'AI ACT classifica ad alto rischio comportano l'adozione di numerosi adempimenti tecnici e organizzativi. Vediamo se è sempre opportuno adottarli o se esistono alternative



Classificazione dei sistemi di IA e pratiche di IA vietate



Strumenti ufficiali



https://ai-act-service-desk.ec.europa.eu/it

Classificazione dei sistemi di IA e pratiche di IA vietate

Seguendo un approccio "basato sul rischio", in base al quale tanto maggiore è il rischio, quanto più rigorose sono le regole, la nuova disciplina stabilisce obblighi per fornitori e operatori dei sistemi di IA a seconda del livello di rischio che l'IA può generare:

i) un rischio inaccettabile;

ii) un rischio alto;

iii) un rischio basso o minimo.

Sono stabiliti anche obblighi specifici per la trasparenza.

Pratiche di IA vietate per rischio inaccettabile

Saranno vietati i sistemi di IA che determinano un rischio inaccettabile per la sicurezza, i mezzi di sussistenza e i diritti delle persone. In questa categoria rientrano i sistemi che **possono manipolare il comportamento umano** come quelli che consentono di attribuire un "punteggio sociale" (social scoring), per finalità pubbliche e private, classificando le persone in base al loro comportamento sociale o alle loro caratteristiche personali, e **determinate applicazioni di polizia predittiva.**

Divieti

Saranno quindi vietati, in particolare:

- i sistemi di **sfruttamento delle vulnerabilità delle persone** e di utilizzo di **tecniche subliminali** ovvero deliberatamente manipolative o ingannevoli;
- i sistemi di **categorizzazione biometrica** delle persone fisiche sulla base di dati biometrici per dedurne o desumerne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale (sarà ancora possibile filtrare set di dati basandosi su dati biometrici nel settore delle attività di contrasto);
- i sistemi di **identificazione biometrica in tempo reale in spazi accessibili al pubblico** (ossia il riconoscimento facciale mediante telecamere a circuito chiuso) da parte delle autorità di contrasto (con limitate eccezioni: vedi oltre);

Divieti

- i **sistemi di riconoscimento delle emozioni** utilizzati sul **luogo di lavoro e negli istituti scolastici**, eccetto per motivi medici o di sicurezza (ad esempio il monitoraggio dei livelli di stanchezza di un pilota);
- l'estrazione non mirata **(scraping) di immagini facciali da internet o telecamere a circuito chiuso** per la creazione o l'espansione di banche dati;
- i sistemi che consentono di attribuire un "**punteggio sociale**" (social scoring), classificando o valutando le persone in base al loro comportamento sociale o alle loro caratteristiche personali.

Divieti - integrazioni

2. Nuovi Divieti Assoluti in Materia di Pratiche di IA (Articolo 5)
Il perimetro delle pratiche vietate (Capo II) viene esteso dal **2 dicembre 2026** a due nuove e gravissime fattispecie di reato digitale:
Generazione o manipolazione di materiale intimo non consensuale (Art. 5, par. 1, lett. b bis): Vieta l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che producono immagini, video o audio realistici delle parti intime di una persona fisica riconoscibile o che la ritraggono in atti sessualmente espliciti senza il suo esplicito consenso.
Generazione o manipolazione di materiale di abuso sessuale su minori (CSAM) (Art. 5, par. 1, lett. b ter): Vieta in modo assoluto i sistemi che generano o manipolano spettacoli o materiale pedopornografico (anche se parzialmente o interamente sintetico).
Criterio di Responsabilità e Misure di Sicurezza (Art. 5, par. 1 bis): Il divieto per i fornitori scatta se la generazione è la finalità prevista o se essa costituisce un risultato ragionevolmente prevedibile e riproducibile in assenza di adeguate misure tecniche di prevenzione (es. *refusal training*, *guardrail*, filtri di output e meccanismi di *red-teaming*). L'uso è vietato in capo al deployer solo se agisce con l'intenzione specifica di generare o manipolare tale materiale.

Sistemi ad alto rischio (art. 6)

Due casistiche specifiche che rimandano agli allegato I e III.

Allegato I - Elenco della normativa di armonizzazione dell'Unione

Allegato III - Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

- settori
- casi d’uso

Esclusioni

Sistemi ad alto rischio (art. 6)

Il regolamento considera ad **alto rischio** un numero limitato di sistemi di IA che possono potenzialmente **avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali** (tutelati dalla Carta dei diritti fondamentali dell'UE).

Prima di immettere un sistema di IA ad alto rischio sul mercato dell'UE, **o di farlo entrare in servizio**, i fornitori dovranno sottoporlo a una **valutazione della conformità**. Dovranno, quindi, **dimostrare che il loro sistema è conforme ai requisiti obbligatori per un'IA affidabile (**ad esempio: qualità dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, accuratezza, cibersicurezza e robustezza). Anche **per i sistemi biometrici** è sempre richiesta una **valutazione della conformità da parte di terzi**. La **valutazione dovrà essere ripetuta in caso di modifica sostanziale del sistema o della sua finalità**.

Sistemi ad alto rischio

I sistemi di IA ad alto rischio dovranno essere **tecnicamente robusti** per garantire che la tecnologia sia adatta allo scopo e che i **risultati falsi positivi/negativi non incidano in modo sproporzionato sui gruppi protetti** (ad esempio, per origine razziale o etnica, sesso, età, ecc.). Dovranno, inoltre, essere **addestrati e testati con set di dati sufficientemente rappresentativi** per ridurre al minimo il rischio di integrare **distorsioni inique** nel modello e garantire che, se presenti, queste possano essere **risolte mediante opportune misure di rilevazione, correzione e attenuazione**. Dovranno anche essere **tracciabili e verificabili**, garantendo la **conservazione dell'opportuna documentazione**, compresi i **dati utilizzati per addestrare l'algoritmo**, fondamentali per le indagini ex post.

Sistemi ad alto rischio

Si impone inoltre agli operatori che siano organismi di diritto pubblico o operatori privati che **forniscono servizi pubblici**, nonché agli **operatori che forniscono sistemi ad alto rischio** di effettuare una **valutazione d'impatto sui diritti fondamentali**.

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

Sistemi ad alto rischio

I sistemi di IA che costituiscono **componenti di sicurezza di prodotti disciplinati dalla legislazione settoriale** dell'Unione saranno **sempre considerati ad alto rischio**, **se soggetti a una valutazione della conformità da parte di terzi ai sensi della legislazione settoriale stessa.** I fornitori di tali sistemi dovranno inoltre attuare sistemi di **gestione della qualità e del rischio** per garantire la conformità ai nuovi requisiti e ridurre al minimo i rischi per gli utenti e per le persone interessate, anche dopo l'immissione sul mercato di un prodotto.

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

Sistemi ad alto rischio

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

Sistemi ad alto rischio

Tra i sistemi ad alto rischio rientrano, in particolare, quelli:

- di **identificazione biometrica remota, categorizzazione biometrica** e **riconoscimento delle emozioni** (al di fuori delle categorie vietate);
- utilizzati come **componenti di sicurezza** nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale e della fornitura di acqua, gas, riscaldamento ed elettricità;
- finalizzati a **determinare l'accesso**, l'ammissione o l'assegnazione agli **istituti di istruzione e formazione professionale** (ad esempio, per valutare i risultati dell'apprendimento e orientare il processo di apprendimento e il monitoraggio dei comportamenti disonesti);
- relativi alla **valutazione dell'occupazione**, ad ottimizzare la gestione dei lavoratori e l'accesso al lavoro autonomo (ad esempio, per pubblicare annunci di lavoro mirati, analizzare e filtrare le candidature e valutare i candidati);
- usati per determinare **l'accesso a servizi e a prestazioni pubblici e privati essenziali** (come, ad esempio, l'assistenza sanitaria);

Sistemi ad alto rischio

finalizzati alla valutazione **dell'affidabilità creditizia** delle persone fisiche, alla **valutazione dei rischi finanziari**, nonché alla **determinazione dei prezzi in relazione ad assicurazioni sulla vita e assicurazioni sanitarie**;

utilizzati nelle **attività di contrasto**, di gestione della **migrazione**, dell'asilo e del controllo delle frontiere, di **amministrazione della giustizia**, nonché nello **svolgimento dei processi democratici** e per la valutazione e **classificazione delle chiamate di emergenza.**

Non sono invece inclusi i sistemi di raccomandazione delle piattaforme online di dimensioni molto grandi (utilizzati dalle aziende online per suggerire agli utenti prodotti, servizi o contenuti che potrebbero essere di loro interesse) in quanto sono già disciplinati da altre normative (regolamento sui mercati digitali e regolamento sui servizi digitali).

L'elenco dei sistemi di IA ad alto rischio, che può essere modificato per allineare la normativa all'evoluzione tecnologica, **è allegato al regolamento**.

Sistemi ad alto rischio - integrazioni

«1 bis.Ai fini del presente regolamento, compreso il paragrafo 1 del presente articolo, i sistemi di IA utilizzati esclusivamente per aspetti non legati alla sicurezza come assistenza agli utenti, ottimizzazione delle prestazioni, efficienza dei servizi, automazione o praticità o controllo della qualità non sono considerati componenti di sicurezza.

1 ter.In deroga al paragrafo 1 bis, i sistemi di IA il cui guasto o malfunzionamento metterebbe a rischio la salute e la sicurezza sono considerati componenti di sicurezza.

1 quater.Un prodotto che deve essere sottoposto a una valutazione della conformità da parte di terzi esclusivamente a causa di rischi diversi da quelli per la salute e la sicurezza, in particolare i rischi relativi alla distribuzione dello spettro radio o alle interferenze elettromagnetiche che non incidono sulla salute e sulla sicurezza, non è considerato conforme alla condizione di cui al paragrafo 1, lettera b).»;

Sistemi ad alto rischio - esclusioni

3.In deroga al paragrafo 2, un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale.
Il primo comma si applica quando è soddisfatta almeno una qualsiasi delle condizioni seguenti:
a) il sistema di IA è destinato a eseguire un compito procedurale limitato;
b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata;
c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; o
d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.

Fatto salvo il primo comma, un sistema di IA di cui all'allegato III è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche.

Sistemi ad alto rischio
Casi di uso e AI generativa

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:

….

b) i sistemi di IA destinati a essere utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro.

Sistemi ad alto rischio

High-risk Artificial Intelligence Systems (Title III, Annexes II and III)



Certain applications in the following fields:

1 **SAFETY COMPONENTS OF REGULATED PRODUCTS**

(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation

2 **CERTAIN (STAND-ALONE) AI SYSTEMS IN THE FOLLOWING FIELDS**

- ✓ Biometric identification and categorisation of natural persons
- ✓ Management and operation of critical infrastructure
- ✓ Education and vocational training
- ✓ Employment and workers management, access to self-employment
- ✓ Access to and enjoyment of essential private services and public services and benefits
- ✓ Law enforcement
- ✓ Migration, asylum and border control management
- ✓ Administration of justice and democratic processes

European Commission

Sistemi ad alto rischio

Requirements for high-risk AI (Title III, chapter 2)



Establish and implement **risk management** processes

&

In light of the **intended purpose** of the AI system

- Use high-quality **training, validation and testing data** (relevant, representative etc.)
- Establish **documentation** and design logging features (traceability & auditability)
- Ensure appropriate certain degree of **transparency** and provide users with **information** (on how to use the system)
- Ensure **human oversight** (measures built into the system and/or to be implemented by users)
- Ensure **robustness**, **accuracy** and **cybersecurity**

Make or Buy

8.1 Caso di Studio: Sistema di IA per la Selezione del Personale (HR)

Ipotesi: un'azienda di medie dimensioni valuta l'introduzione di un sistema di IA per lo screening automatizzato dei candidati in fase di selezione del personale (Allegato III, punto 4, lett. a, AI Act). Orizzonte di valutazione: n = 3 anni. Fatturato annuo dell'organizzazione: € 40.000.000.

8.2 Confronto C_sistema

Voce	MAKE (€, 3 anni)	BUY (€, 3 anni)
R&D / Licenze SaaS	250.000	180.000
Data ingestion/labeling / Integrazione API	90.000	45.000
Compute-GPU / Customizzazione	90.000	30.000
Stipendi Data Scientist / Canoni di supporto	540.000	45.000
Manutenzione ed evoluzione architetturale	120.000	-
TOTALE C_sistema	1.090.000	300.000

8.3 Confronto C_compliance

Voce	MAKE (€, 3 anni)	BUY (€, 3 anni)
Obblighi ex-ante/post-market (MAKE) o da Deployer (BUY)	320.000	92.000
Normative trasversali (GDPR, PLD, NIS2/DORA, sicurezza lavoro)	70.000	70.000
TOTALE C_compliance	390.000	162.000

Make or Buy

8.7 Matrice Decisionale Multicriterio Applicata

Punteggi attribuiti (1=sfavorevole, 5=favorevole), in ragione delle specificità del caso: assenza di vantaggio competitivo distintivo nello screening HR, pressione a un rilascio rapido, capability interne di data science non ancora consolidate.

Criterio	Peso	Punteggio MAKE	Punteggio BUY
TCO Rettificato al Rischio	35%	2	5
Time-to-Market	20%	1	5
Controllo su IP e vantaggio competitivo	15%	5	1
Capability interne di AI Governance	15%	2	4
Soglia di accettabilità del rischio	15%	2	4
PUNTEGGIO PONDERATO TOTALE	100%	2,25	4,10

VERDETTO: BUY

TCO_BUY (€ 501.070) è nettamente inferiore a TCO_MAKE (€ 1.611.600) e il punteggio ponderato multicriterio conferma la convergenza (BUY 4,10 vs MAKE 2,25 su 5). Le due valutazioni sono concordanti → esito BUY, subordinato alla negoziazione di clausole contrattuali di manleva rafforzate e a un audit di conformità del fornitore prima della firma.

Obblighi di trasparenza per finalità generali

A determinati sistemi di IA sono imposti specifici obblighi di trasparenza, ad esempio laddove esista un evidente rischio di manipolazione (come attraverso l'uso di **chatbot**); gli **utenti dovranno essere consapevoli del fatto che stanno interagendo con una macchina**. I fornitori di sistemi di IA, compresi i sistemi di IA per finalità generali (**General purpose AI - GPAI**), che **generano contenuti audio, immagini, video o di testo sintetici**, dovranno garantire che **i risultati del sistema di IA siano contrassegnati in un formato leggibile dalla macchina e rilevabili come generati o manipolati artificialmente.**

Anche i **deep fake dovranno essere etichettati come tali** e gli **utenti dovranno essere informati quando vengono utilizzati sistemi di categorizzazione biometrica o di riconoscimento delle emozioni.**

Sistemi a rischio minimo

I sistemi di IA a **rischio minimo** (come **videogiochi o filtri spam**) saranno esenti da obblighi, ferma restando l'**adesione volontaria a codici di condotta**, da parte dei fornitori di tali sistemi, ad esempio laddove esista un evidente rischio di manipolazione. **Gli utenti dovranno essere consapevoli del fatto che stanno interagendo con una macchina.**

La grande maggioranza dei sistemi di IA attualmente utilizzati o il cui utilizzo è probabile nell'UE rientra in questa categoria.

Rischi sistemici

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

Il "**rischio sistemico** a livello di Unione" si riferisce alla possibilità che l'uso dell'IA possa avere un **impatto significativo sul mercato interno a causa della sua portata e con effetti negativi reali o ragionevolmente prevedibili su salute pubblica, sicurezza, diritti fondamentali** o sulla società nel suo insieme, che possono essere propagati su larga scala lungo tutta la catena del valore. Ad esempio, **se un'applicazione di guida autonoma mal funzionasse su larga scala, potrebbe causare incidenti stradali su vasta scala, influenzando quindi l'intero sistema di mobilità urbana**.

Incidente grave

Quanto al concetto di “incidente grave”, ci si riferisce a **qualsiasi incidente o malfunzionamento di un sistema di IA che porti direttamente o indirettamente a uno dei seguenti effetti:**

(a) **la morte di una persona o un grave danno alla salute di una persona**;

b) un'**interruzione grave e irreversibile** della **gestione e del funzionamento delle infrastrutture critiche**;

c) **violazione degli obblighi derivanti dal diritto dell'Unione volti a tutelare i diritti fondamentali**;

d) **danni gravi alla proprietà o all'ambiente**.

Ad esempio, si pensi ad un errore in un sistema diagnostico medico basato sull'IA che porta a diagnosi errate e danni significativi ai pazienti

Codici di condotta

L'Ufficio per l'IA incoraggia e facilita l'elaborazione di codici di condotta a livello di Unione per **facilitare l'efficace attuazione degli obblighi in materia di rilevamento ed etichettatura di contenuti generati o manipolati artificialmente.**

Eccezioni previste per le autorità di contrasto

L’uso dell'IA da parte delle forze dell’ordine ha rappresentato uno dei punti più delicati e controversi del negoziato. Il compromesso raggiunto consente il **riconoscimento biometrico da remoto in tempo reale negli spazi accessibili al pubblico solo in alcuni casi quali:**

1) attività di contrasto relative a 16 reati specifici:

- terrorismo;
- tratta di esseri umani;
- sfruttamento sessuale di minori e materiale pedopornografico;
- traffico illecito di stupefacenti e sostanze psicotrope;
- traffico illecito di armi, munizioni ed esplosivi;

Eccezioni previste per le autorità di contrasto

- omicidio volontario;
- lesioni personali gravi;
- traffico illecito di organi e tessuti umani;
- traffico illecito di materie nucleari e radioattive,
- rapimento, sequestro e presa di ostaggi;
- reati che rientrano nella competenza giurisdizionale della Corte penale internazionale;
- dirottamento di un aeromobile o una nave;
- stupro;
- reati ambientali;
- furto organizzato o rapina a mano armata;
- sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra;

Eccezioni previste per le autorità di contrasto

2**) ricerca mirata di specifiche vittime**, rapimento, tratta e sfruttamento sessuale di esseri umani e persone scomparse;

3) **prevenzione di minacce per la vita o l'incolumità fisica delle persone** o risposta da una minaccia attuale o prevedibile di **attacco terroristico**.

Eccezioni previste per le autorità di contrasto

L'identificazione biometrica remota in tempo reale da parte delle autorità di contrasto sarà **subordinata a un'autorizzazione preventiva** rilasciata da un'autorità giudiziaria o amministrativa indipendente. In caso di urgenza debitamente giustificata, tuttavia, si potrà procedere senza un'autorizzazione, purché quest'ultima sia richiesta senza indebito ritardo, al più tardi entro 24 ore; se l'autorizzazione non è concessa, è necessario che tutti i dati e gli output siano soppressi. L'autorizzazione dovrà essere **preceduta da una valutazione preventiva d'impatto sui diritti fondamentali** e dovrà essere notificata all'autorità di vigilanza e all'autorità per la protezione dei dati interessate.

Sistemi di IA per finalità generali e modelli fondativi o di base

La nuova disciplina, introdotta nell'accordo di compromesso finale, su richiesta del PE, reca disposizioni dettagliate applicabili alle situazioni in cui i **sistemi di IA per finalità generali** (general purpose AI) sono **utilizzati per scopi per i quali non sono stati intenzionalmente e specificamente progettati** e in cui la tecnologia viene **successivamente integrata in un altro sistema ad alto rischio**. I modelli di IA per finalità generali comprendono i modelli di IA generativa di grandi dimensioni.

Sistemi di IA per finalità generali e modelli fondativi o di base

È considerato importante che un fornitore che intenda basarsi su un modello di IA per finalità generali disponga di tutte le informazioni necessarie per far sì che il suo sistema sia sicuro e conforme al regolamento. **Il regolamento obbliga i fornitori di tali modelli a comunicare determinate informazioni ai fornitori di sistemi a valle**. I fornitori dovranno inoltre disporre di politiche in essere atte a garantire il rispetto del diritto d'autore nel corso della formazione dei loro modelli.

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

La Commissione europea ritiene che, allo stato attuale della tecnologia, i modelli di IA per finalità generali che sono stati addestrati utilizzando una potenza di calcolo totale superiore a 10^25 FLOPS comportino rischi sistemici.

Misure a sostegno dell'innovazione

Il regolamento contiene diverse misure a sostegno dell'innovazione. In particolare, consente la **creazione di spazi di sperimentazione normativa per l'IA (sandbox normativi)** e di **prova in condizioni reali, che forniscono un ambiente controllato** per testare tecnologie innovative per un periodo di tempo limitato, promuovendo in tal modo l'innovazione da parte delle imprese, delle PMI e delle start-up.

Gli Stati membri dovranno istituire almeno un sandbox normativo sull'IA a livello nazionale. Potrà anche essere istituito congiuntamente tra più Stati membri.

Misure a sostegno dell'innovazione

Le prove in condizioni reali dei sistemi di IA ad alto rischio potranno essere **effettuate per un massimo di 6 mesi (prorogabili di altri 6 mesi). Prima delle prove dovrà essere elaborato un piano da presentare all'autorità di vigilanza del mercato**, la quale dovrà approvare il piano e le condizioni di prova specifiche; in caso di mancata risposta entro 30 giorni, il piano si considererà tacitamente approvato. **Le prove potranno essere oggetto di ispezioni senza preavviso da parte dell'Autorità.**

Misure a sostegno dell'innovazione

Le prove in condizioni reali potranno essere effettuate **solo se sono presenti garanzie specifiche**: ad esempio, gli utenti dei sistemi sottoposti a prova in condizioni reali dovranno fornire **un consenso informato**, **le prove non dovranno avere alcun effetto negativo** sugli utenti, gli esiti delle prove dovranno essere reversibili o poter essere ignorati, **i relativi dato dovranno essere cancellati** dopo la conclusione delle prove. Una protezione speciale dovrà essere riservata ai gruppi vulnerabili, ad esempio a causa della loro età o della disabilità fisica o mentale.

Architettura di governance

Le **autorità nazionali** competenti per la vigilanza del mercato sorveglieranno l'attuazione delle nuove norme a livello nazionale, mentre un **Ufficio europeo per l'IA**, costituito presso la Commissione europea, garantirà il coordinamento a livello europeo. Ciascuno Stato membro designerà una o più autorità nazionali competenti, incaricate di supervisionarne l'applicazione e l'attuazione, nonché di svolgere attività di vigilanza del mercato.

Un **comitato scientifico di esperti indipendenti** avrà il compito di segnalare i rischi sistemici e contribuire alla classificazione e alla sperimentazione dei modelli. Un **comitato europeo per l'IA**, composto dai rappresentanti degli Stati membri, svolgerà il ruolo di piattaforma di coordinamento e di organo consultivo per la Commissione europea. Il Garante europeo della protezione dei dati parteciperà come osservatore.

Architettura di governance

Si prevede infine l'istituzione di un **forum consultivo per i portatori di interessi**, come i rappresentanti dell'industria, le PMI, le start-up, la società civile e il mondo accademico.

Sistemi di IA già immessi sul mercato o messi in servizio

Per quanto riguarda i sistemi di IA già immessi sul mercato o messi in servizio, l'accordo di compromesso stabilisce in particolare che: **le autorità pubbliche che sono fornitori o utilizzatori di sistemi di IA ad alto rischio avranno quattro anni** di tempo per rendere conformi i propri sistemi; **i modelli GPAI** immessi sul mercato prima della data di applicazione delle disposizioni a loro relative (ossia 12 mesi dopo l'entrata in vigore del regolamento) avranno **due anni** di tempo dalla data di applicazione di tali disposizioni (quindi 3 anni in totale) per conformarsi.

Sanzioni

Le sanzioni per le violazioni del nuovo regolamento sono state fissate in una percentuale del fatturato annuo globale nell'anno finanziario precedente della società incriminata o in un importo predeterminato, a seconda di quale sia il più elevato.

Più nello specifico, per i sistemi di IA che sono immessi sul mercato o messi in servizio e che non rispettano i requisiti del regolamento, gli Stati membri dovranno stabilire sanzioni effettive, proporzionate e dissuasive, comprese sanzioni amministrative pecuniarie, in relazione alle violazioni, e comunicarle alla Commissione. Il regolamento stabilisce le soglie da tenere in considerazione:

fino a 35 milioni di euro o al 7% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore) per violazioni relative a pratiche vietate o per l'inosservanza di requisiti in materia di dati;

Sanzioni

fino a 15 milioni di euro o al 3% del fatturato mondiale totale annuo dell'esercizio precedente, per l'inosservanza di qualsiasi altro requisito o obbligo del regolamento, compresa la violazione delle regole relative ai modelli di IA per finalità generali;

fino a 7,5 milioni di euro o all'1,5% del fatturato mondiale totale annuo dell'esercizio precedente, per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti in risposta a una richiesta;

per ciascuna categoria di violazione, la soglia per le PMI sarebbe l'importo più basso tra i due previsti, mentre per le altre imprese sarebbe l'importo più elevato.

Documenti integrativi

Pubblicati

https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

In sviluppo

In the course of 2026, the Commission will develop:

- Guidelines on the practical application of the high-risk classification
- Guidelines on the practical application of the transparency requirements under Article 50 AI Act
- Guidance on the reporting of serious incidents by providers of high-risk AI systems
- Guidelines on the practical application of the high-risk requirements
- Guidelines on the practical application of the obligations for providers and deployers of high-risk AI systems
- Guidelines with a template for the fundamental rights impact assessment
- Guidelines on the practical application of rules for responsibilities along the AI value chain
- Guidelines on the practical application of the provisions related to substantial modification
- Guidelines providing a voluntary template for the post-market monitoring of high-risk AI systems
- Guidelines on the elements of the quality management system which SMEs and SMCs may comply with in a simplified manner
- Guidelines on the AI Act's interplay with other EU legislation, for example the joint guidelines of the Commission and European Data Protection Board on the interplay of the AI Act and EU data protection law

Documenti integrativi

- The Guidelines on the scope of the obligations for providers of GPAI models clarify the scope of the GPAI obligations under the AI Act, helping actors along the AI value chain understand who must comply with these obligations.
- The GPAI Code of Practice is a voluntary compliance tool submitted to the Commission by independent experts, which offers practical guidance to help providers comply with their obligations under the AI Act related to transparency, copyright, and safety & security.
- The Template for the public summary of training content of GPAI models requires providers to give an overview of the data used to train their models. This includes the sources from which the data was obtained (comprising large datasets and top domain names).The template also requests information about data processing aspects to enable parties with legitimate interests to exercise their rights under EU law.
- The Code of Practice on marking and labelling of AI-generated content selected by the AI Office. The code will be a voluntary tool to guide providers and deployers of generative AI systems to comply with transparency obligations. These include marking AI generated content and disclosing the artificial nature of images, and audio (including deepfakes) as well as text.
- The Guidelines on transparent AI systems to clarify the scope of application, relevant legal definitions, the transparency obligations, the exceptions and related horizontal issues.
- The guidelines on prohibited AI practices under the AI Act, which offer legal explanations and practical examples to help stakeholders understand and comply with the prohibitions.
- The guidelines on the AI system definition of the AI Act, to assist stakeholders in determining the scope of the AI Act

Documenti integrativi

Orientamenti sulla classificazione dei sistemi ad alto rischio

Art. 6, par. 5.

Specificano l'attuazione pratica dei criteri di classificazione per i sistemi di IA ad alto rischio, corredati da un elenco esaustivo di esempi pratici di casi d'uso (sia ad alto rischio che non).

Modulo di documentazione tecnica semplificata per le PMI

Art. 11, par. 1.

Un modello semplificato volto a rispondere alle esigenze delle piccole e microimprese (comprese le start-up) per la redazione della documentazione tecnica obbligatoria, accettabile dagli organismi notificati ai fini della valutazione della conformità.

Modello di questionario per la FRIA (Valutazione d'impatto sui diritti fondamentali)

Art. 27, par. 5.

Un questionario, disponibile anche tramite strumento automatizzato, progettato per agevolare i deployer (utilizzatori) nell'adempimento dell'obbligo di effettuare la valutazione d'impatto sui diritti fondamentali in modo semplificato.

4. Modello per la sintesi dei contenuti di addestramento dei modelli GPAI

Art. 53, par. 1, lett. d).

Uno schema standardizzato che i fornitori di modelli di IA per finalità generali (GPAI) devono utilizzare per mettere a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti usati per l'addestramento dei loro modelli.

Codici di buone pratiche (Codes of Practice)

Art. 56, par. 1 e 9.

Documenti volti a contribuire alla corretta applicazione del regolamento per i fornitori di modelli GPAI. Devono coprire obblighi di trasparenza, aggiornamento delle informazioni tecniche e gestione dei rischi sistemici.

Documenti integrativi

Modalità dettagliate per gli spazi di sperimentazione normativa (Sandboxes)

Art. 58, par. 1

Atti di esecuzione che precisano i criteri di ammissibilità, le procedure di domanda, monitoraggio e uscita dagli spazi di sperimentazione normativa per l'IA.

Specifiche del piano di prova in condizioni reali

Art. 60, par. 1

Atti di esecuzione che definiscono nel dettaglio gli elementi che devono comporre il piano di prova per i sistemi testati al di fuori degli spazi di sperimentazione.

Modelli standardizzati settoriali

Art. 62, par. 3, lett. a).

Modelli standardizzati per i diversi settori disciplinati dal regolamento, forniti su richiesta del comitato per l'IA, per supportare in particolare le PMI nello sviluppo di sistemi conformi.

Orientamenti per le microimprese sul sistema di gestione della qualità (SGQ)

Art. 63, par. 1

Linee guida che specificano quali elementi del SGQ possono essere soddisfatti in modo semplificato dalle microimprese senza compromettere il livello di sicurezza.

Documenti integrativi

Modello per il piano di monitoraggio post-commercializzazione

Art. 72, par. 3.

Un modello che definisce gli elementi minimi da includere nel piano di monitoraggio successivo all'immissione sul mercato per i sistemi di IA ad alto rischio.

Orientamenti sulla segnalazione di incidenti gravi

Art. 73, par. 7.

Linee guida specifiche per facilitare i fornitori nel rispetto degli obblighi di notifica alle autorità di vigilanza in caso di incidenti gravi o malfunzionamenti dei sistemi di IA.

9. Orientamenti generali sull'attuazione pratica del Regolamento

Art. 96, par. 1.

Una guida onnicomprensiva che copre:

- l'applicazione dei requisiti e degli obblighi di cui agli articoli da 8 a 15 e all'articolo 25;
- le pratiche vietate di cui all'articolo 5;
- l'attuazione pratica delle disposizioni relative alla modifica sostanziale;
- l'attuazione pratica degli obblighi di trasparenza di cui all'articolo 50;
- informazioni dettagliate sulla relazione del presente regolamento con la normativa di armonizzazione dell'Unione elencata nell'allegato I, nonché con altre disposizioni pertinenti di diritto dell'Unione, anche per quanto riguarda la coerenza nella loro applicazione;
- l'applicazione della definizione di sistema di IA di cui all'articolo 3, punto 1).

Documenti integrativi

Specifiche funzionali della banca dati dell'UE

Art. 71, par. 1.

Documentazione tecnica e operativa relativa alla struttura, al funzionamento e alle modalità di registrazione delle informazioni nella banca dati dell'UE per i sistemi di IA ad alto rischio.

Specifiche sulle garanzie procedurali per le sanzioni (GPAI)

Art. 101, par. 6

Atti di esecuzione che stabiliscono le modalità per i procedimenti e le garanzie procedurali relative alle sanzioni pecuniarie per i fornitori di modelli GPAI.

Valutazione annuale dell'Allegato III e dell'Articolo 5

Art. 112, par. 1

La Commissione deve valutare ogni anno la necessità di modificare l'elenco dei sistemi ad alto rischio e delle pratiche vietate.

Relazione di valutazione e riesame quadriennale

Art. 112, par. 3, 4, 6

Un rapporto dettagliato al Parlamento e al Consiglio che valuta l'efficacia del sistema di governance, lo stato delle sanzioni, l'impatto sulle PMI e i progressi della normazione tecnica.

Valutazione del funzionamento dell'Ufficio per l'IA

Art. 112, par. 5

Un'analisi specifica sui poteri e sulle risorse dell'Ufficio per l'IA da presentare entro il 2 agosto 2028.

Uso dell'AI generativa

- Attività preliminari:
  - Identificazione
  - Censimento
  - Classificazione
- Implementazione dei requisiti normativi
- Audit



- https://iterdigital.it/it_it/ai-act-in-pratica/
- https://iterdigital.it/it_it/download/154043/
- https://www.cybersecurity360.it/legal/luso-dellai-generativa-come-supporto-alla-conformita-normativa/

INDICE

INDICE ..... *v*

GUIDA ALLA LETTURA DI QUESTO LIBRO ..... *ix*
- Finalità e struttura del libro ix
- AVVERTENZE SUL CONTENUTO GENERATO DALL'AI ix
- Ambito e approccio x
- Rappresentazione del contenuto del testo xi
- Revisione del testo xi

USO DEGLI STRUMENTI DI AI GENERATIVA *1*
- Claude 2
- Uso di CLAUDE e strumenti analoghi 5
- Uso di Gemini NoteBook 6
- Perché è opportuno usare contemporaneamente diversi strumenti 7
- Esempio di uso combinato di più strumenti 8
- Uso di Genspark per interrogazioni multiple 10
- Limiti nell'uso degli strumenti di AI generativa 10
- Anonimizzare il contenuto dei documenti 10
- I consigli dell'AI per anonimizzare il contenuto dei documenti 12
- Uso di modelli di AI in locale 18
- Uso di versioni aziendali di sistemi di AI generativa 21

CREARE PROMPT EFFICACI *23*
- Richiedere agli strumenti come creare un prompt efficace 23
- Creazione e ottimizzazione dei prompt direttamente da parte degli strumenti 49
- Generazione di prompt con uso di strumenti AI partendo da modelli 54
- Buone pratiche per la generazione di prompt 59
- Paradigmi dell'uso dell'AI generativa 59

L'USO DELL' AI IN AZIENDA *61*
- Definizione di AI 61
- Policy aziendale sull'AI generativa 61
- Policy per l'uso dell'AI in azienda 65
- Ruoli e responsabilità 77
- Procedura per l'implementazione di un sistema di AI 81
- Sviluppo di un sistema di AI ad alto rischio: valutazione MAKE or BUY 98

AI ACT: ASPETTI NORMATIVI *113*
- Composizione della normativa sull'AI 113

- Regolamentazione internazionale e comparata 113
- Architettura del Regolamento AI Act 115
- Principi dell'AI Act 121
- Strumenti ufficiali 124
- Ambito di applicazione 124
- Identificazione di un sistema/modello di AI 128
- AI Act e altre normative UE 133

CLASSIFICAZIONE DEI SISTEMI *151*
- Classificazione dei sistemi AI 151
- Classificazione dei modelli AI 153
- Sistemi di AI per finalità previste e per finalità generali 155
- Sistemi vietati capo II art. 5 157
- Sistemi a rischio alto - capo III art. 6 163
- Eccezioni all'alto rischio 176
- Sistemi con requisiti di trasparenza 177
- Sistemi a rischio minimo 181

ADEMPIMENTI DI CARATTERE GENERALE *183*
- Mappatura, identificazione e classificazione dei sistemi/modelli di AI 183
- Mappatura 184
- Verifica che un sistema sia un sistema AI ai sensi dell'AI ACT 194
- Classificazione 200
- Formazione 210
- Trattamento di categorie particolari di dati personali ai fini del rilevamento e della correzione delle distorsioni 213

ADEMPIMENTI PER LIVELLO DI RISCHIO *217*
- Operatori e relativi adempimenti 217

IMPLEMENTAZIONE *239*
- Tutti i sistemi 239
- Sistemi vietati 240
- Sistemi ad alto rischio 242
- Test dei sistemi ad alto rischio 248
- Sistemi con requisiti di trasparenza 251
- Sistemi a rischio minimo 251
- Valutazione della conformità, certificati, registrazione 251
- Modelli di AI per finalità generali 255

CREAZIONE DELLE PROCEDURE DI IMPLEMENTAZIONE *261*
- Esempio 1 – Articolo 9 262
- Esempio 2 - Articolo 8: Conformità ai requisiti 276
- Esempio 3 - Articolo 13: Trasparenza e fornitura di informazioni ai deployer 280
- Esempio 4 - Articolo 15: Accuratezza, robustezza e cibersicurezza 296

AI ACT – © Giancarlo Butti

Esempio 5 - Articolo 17: Sistema di gestione della qualità....299
Esempio 6 - Articolo 18: Conservazione dei documenti....313
Esempio 7 - Articolo 19: Log generati automaticamente....315
Esempio 8 - Articolo 27: Valutazione d'impatto sui diritti fondamentali per i sistemi di AI ad alto rischio....317
Implementazione delle norme di valutazione della conformità, certificati, registrazione....320
Esempio 9 - Articolo 43 : Valutazione della conformità....320
Esempio 10 - Articolo 44 : Certificati....332
Esempio 11 - Articolo 47 : Dichiarazione di conformità UE....335
Esempio 12 - Articolo 48 : Marcatura CE....337
Esempio 13 - Articolo 49 : Registrazione....340
Implementazione degli obblighi di trasparenza per i fornitori e i deployer di determinati sistemi di AI....343
Esempio 14 - Articolo 50 : Obblighi di trasparenza per i fornitori e i deployers di determinati sistemi di IA....343
Implementazione degli obblighi dei fornitori di modelli di AI per finalità generali .355
Esempio 15 - Articolo 53: Obblighi dei fornitori di modelli di IA per finalità generali 355
Esempio 16 - Articolo 55: Obblighi dei fornitori di modelli di IA per finalità generali con rischio sistemico....357

L'AUDIT NELL'AMBITO DELL'AI Act....361
Esempio 1 – Ambiti di audit....361
Tipologie di Audit in ambito AI Act....372
Classificazione per ambito....372
Audit iniziali....378
Audit sulla infrastruttura a supporto dell'AI....383
Audit sull'interazione con altre normative....388
Definizione del piano di audit....389
Esempio 2 – Valutazione delle aree a maggior rischio....389
Esempio 3 – Pianificazione dell'attività di audit sull'AI Act....398

CHECK LIST DI AUDIT....433
Esempio 1 – Articolo 11....433
Esempio 2 – Articoli 8-10....440
Esempio 3 – Articoli 12 – 15....446
Esempio 4 – Articoli 13 e 52 trasparenza....450
Esempio 5 – Valutazione dei fornitori e della ai supply chain....468
Esempio 6 – Articolo 11....477
Esempio 7 – Gestione del ciclo di vita di un sistema AI....482
Esempio 8 - Cybersecurity....487

APPLICAZIONI....493
Sistemi AI ai sensi dell'AI Act....493

Sistemi vietati....500
Sistemi ad alto rischio art. 6.1....505
Sistemi ad alto rischio art. 6.2....508

APPENDICE A: ESEMPI DI AUDIT....511
Audit sulla identificazione di un sistema come sistema di AI....511
Audit sul censimento dei sistemi di AI....523
Audit sulla classificazione dei sistemi di AI....536
Audit sulla dismissione di un sistema vietato....553

FRAMEWORK DI DISCOVERY E INVENTORY ESAUSTIVO DELL'AI AZIENDALE

Mappatura del perimetro "Zero Shadow AI" — checklist, questionario e registro operativo

Perimetro di mappatura — le 6 macro-categorie

- 1. AI Generativa e Produttività (SaaS/Cloud)
- 2. Agenti AI e Automazione dei Processi
- 3. AI Embedded in Software Enterprise (terze parti)
- 4. Componenti/Modelli AI in prodotti e codice interno
- 5. Hardware e IoT con AI on-device
- 6. Shadow AI e Progetti Informali

Il framework è costruito secondo il principio "Zero Shadow AI": ogni fonte di rilevamento è incrociata su più macro-categorie, in modo che l'assenza di un riscontro in una fonte sia compensata dalla verifica incrociata in un'altra (difesa in profondità del censimento).

Fase 1 — Matrice delle Fonti di Rilevamento

Le tre checklist seguenti individuano, per ciascuna funzione aziendale coinvolta, dove e come cercare tracce di AI utilizzata, sviluppata, integrata o testata. Le checklist sono complementari: una funzione da sola non è in grado di intercettare l'intero perimetro.

1.1 Checklist IT & Cybersecurity

N°	Azione di verifica (cosa fare e dove/con quale strumento)	Categorie AI intercettate	Frequenza consigliata
1	Analisi dei log firewall/proxy/DNS alla ricerca di traffico verso domini noti di servizi AI (elenco aggiornato: chatgpt.com, openai.com, anthropic.com, claude.ai, midjourney.com, perplexity.ai, deepl.com, jasper.ai, copy.ai, character.ai, huggingface.co, stability.ai, elevenlabs.io, runwayml.com).	Cat. 1, 4, 6	*Mensile*
2	Estrazione dei report del CASB/SASE (Cloud Access Security Broker) sulle applicazioni SaaS non censite ('Shadow SaaS') e filtro per categoria 'AI/ML'.	Cat. 1, 3, 6	*Mensile*
3	Query sul SIEM per user-agent/header HTTP riconducibili a SDK e librerie AI (es. 'OpenAI-Python', 'LangChain', 'Anthropic-SDK', chiamate verso api.*.ai).	Cat. 2, 4, 6	*Mensile*

Paradigmi dell'uso di strumenti di AI generativa: esperienza personale

1) La propria esperienza con uno strumento non conta nulla

- L'evoluzione degli strumenti è talmente rapida che quello che conosciamo oggi di uno strumento, dei suoi limiti e delle sue potenzialità può essere obsoleto domani.
- Quindi questi strumenti vanno rianalizzati nel continuo per comprendere cosa è meglio utilizzare in un determinato periodo per un uso specifico.
- È consigliabile mantenersi continuamente aggiornati con l'uso di diversi strumenti e seguendo canali di aggiornamento.

Paradigmi dell'uso di strumenti di AI generativa: esperienza personale

2) Come interagire

- Non è necessario conoscere gli strumenti o porsi quesiti in merito a cosa possono servire.
- È sufficiente chiederlo allo strumento stesso.
- Per la prima volta ci si trova di fronte ad applicazioni che guidano l'utente nel loro uso.
- Non è necessario essere esperti per creare prompt efficaci, perché basta chiedere allo stesso strumento di generarli o chiedere come vuole essere interrogato.
- È possibile chiedere qualunque cosa per superare i limiti apparenti dello strumento, ad esempio quali fonti ha utilizzato, qual è stato il suo ragionamento…

Paradigmi dell'uso di strumenti di AI generativa: esperienza personale

3) Gli strumenti non sono affidabili e quindi:

- Vanno usati solo su temi che si padroneggiano
- È utile verificare la risposta di più strumenti
- Vanno individuate strategie per effettuare controlli automatici della validità delle risposte
- Chiedere allo strumento come fare a controllare la risposta

Paradigmi dell'uso di strumenti di AI generativa: esperienza personale

4) Informazioni riservate

- Impostare lo strumento affinché non usi le informazioni caricate per addestrare il modello (se lo consente e si ritiene affidabile il produttore nelle sue affermazioni)
- Anonimizzare le informazioni
- Usare una versione aziendale dei modelli
- Utilizzare modelli in locale

Grazie per l'attenzione

giancarlo.butti@promo.it

gbutti@clusit.it

338 9230742