Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA

SECURITY SUMMIT

Security Summit

Verona, 24 ottobre 2024

AI Act: tutto quello che c'è da sapere (e gli impatti per il mondo cyber)

Gabriele Franco | Avvocato

PANETTA
Consulting Group

Gabriele Franco
Avvocato e Senior Associate,
Panetta Consulting Group

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT
VERONA

ASTREA

PANETTA
Consulting Group

AI Act: tutto quello che c'è da sapere (e gli impatti per il mondo cyber)

24 ottobre 2024

panetta.it

PANETTA studio legale
insAIde
PRIVACY & TECHNOLOGY PROFESSIONALS
strand alliance

PANETTA
Consulting Group

Carta d’identità

- Regolamento UE
- Normativa di prodotto
- Protezione + innovazione
- Risk-based approach

PANETTA
Consulting Group

Iter di approvazione

Aprile 2021

La **Commissione UE** presenta la **proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale**.

Novembre 2021

La Presidenza slovena del **Consiglio dell'UE**, dopo le discussioni **iniziate a luglio**, condivide il **primo testo di compromesso**.

Dicembre 2021

Viene stabilito che le commissioni per il mercato interno (IMCO) e per le libertà civili (LIBE) del **Parlamento europeo** conducono i **negoziati sull'AI Act**, Brando Benifei è il negoziatore principale.

Giugno 2022

La Presidenza francese del **Consiglio dell'UE**, dopo le discussioni **iniziate a gennaio**, condivide il **testo finale di compromesso**.

Aprile 2023

Dopo la presentazione di **migliaia di emendamenti tra aprile 2021 e marzo 2023**, il **Parlamento europeo** raggiunge un **accordo politico provvisorio** sull'AI Act.

Dicembre 2022

La Presidenza ceca del **Consiglio dell'UE** raggiunge un **testo di compromesso**.

Giugno 2023

Si svolge il **voto in plenaria** del **Parlamento europeo** sull'accordo di compromesso sull'AI Act.

Luglio 2023

Inizia il **trilogo** tra le istituzioni UE.

Dicembre 2023

Accordo politico provvisorio.

Marzo 2024

Il Parlamento europeo **approva definitivamente** l'AI Act

Maggio 2024

Il Consiglio dell'UE **approva definitivamente** l'AI Act

Luglio 2024

Pubblicazione in **GUE** e entrata in vigore

Consiglio dell'UE

Parlamento UE

PANETTA
Consulting Group

Oggetto

L'AI Act stabilisce

- Regole **armonizzate** per l'immissione sul mercato, la messa in servizio e l'uso dei **sistemi di IA** nell'UE
- **Divieti** di talune pratiche di IA
- **Requisiti specifici** per i sistemi di IA ad **alto rischio** e **obblighi** per gli operatori di tali sistemi
- Regole di **trasparenza** armonizzate per determinati sistemi di IA
- Regole **armonizzate** per l'immissione sul mercato di **modelli di IA per finalità generali**
- Regole in materia di **monitoraggio** del mercato, **governance** della vigilanza del mercato e applicazione
- Misure a **sostegno dell'innovazione**, con particolare attenzione a **PMI** e **startup**

PANETTA
Consulting Group

Definizione di IA

Commissione UE

«sistema di intelligenza artificiale»: un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono.

Consiglio dell'UE

«sistema di intelligenza artificiale»: un sistema progettato per funzionare con elementi di autonomia e che, sulla base di dati e input forniti da macchine e/o dall'uomo, deduce come raggiungere una determinata serie di obiettivi avvalendosi di approcci di apprendimento automatico e/o basati sulla logica e sulla conoscenza, e produce output generati dal sistema quali contenuti (sistemi di IA generativa), previsioni, raccomandazioni o decisioni, che influenzano gli ambienti con cui il sistema di IA interagisce.

Parlamento europeo

«sistema di intelligenza artificiale»: un sistema automatizzato progettato per operare con livelli di autonomia variabili e che, per obiettivi espliciti o impliciti, può generare output quali previsioni, raccomandazioni o decisioni che influenzano gli ambienti fisici o virtuali.

a) approcci di apprendimento automatico, compresi l'apprendimento supervisionato, non supervisionato e per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (deep learning);
b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti;
c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.

AI Act

«**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.

PANETTA
Consulting Group

Ruoli

FORNITORE

Una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo **che sviluppa un sistema di IA o che fa sviluppare un sistema di IA al fine di immetterlo sul mercato o metterlo in servizio con il proprio nome o marchio**, a titolo oneroso o gratuito.

DEPLOYER

Qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che **utilizza un sistema di IA sotto la sua autorità**, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale.

PANETTA
Consulting Group

Campo di applicazione

Si applica a:

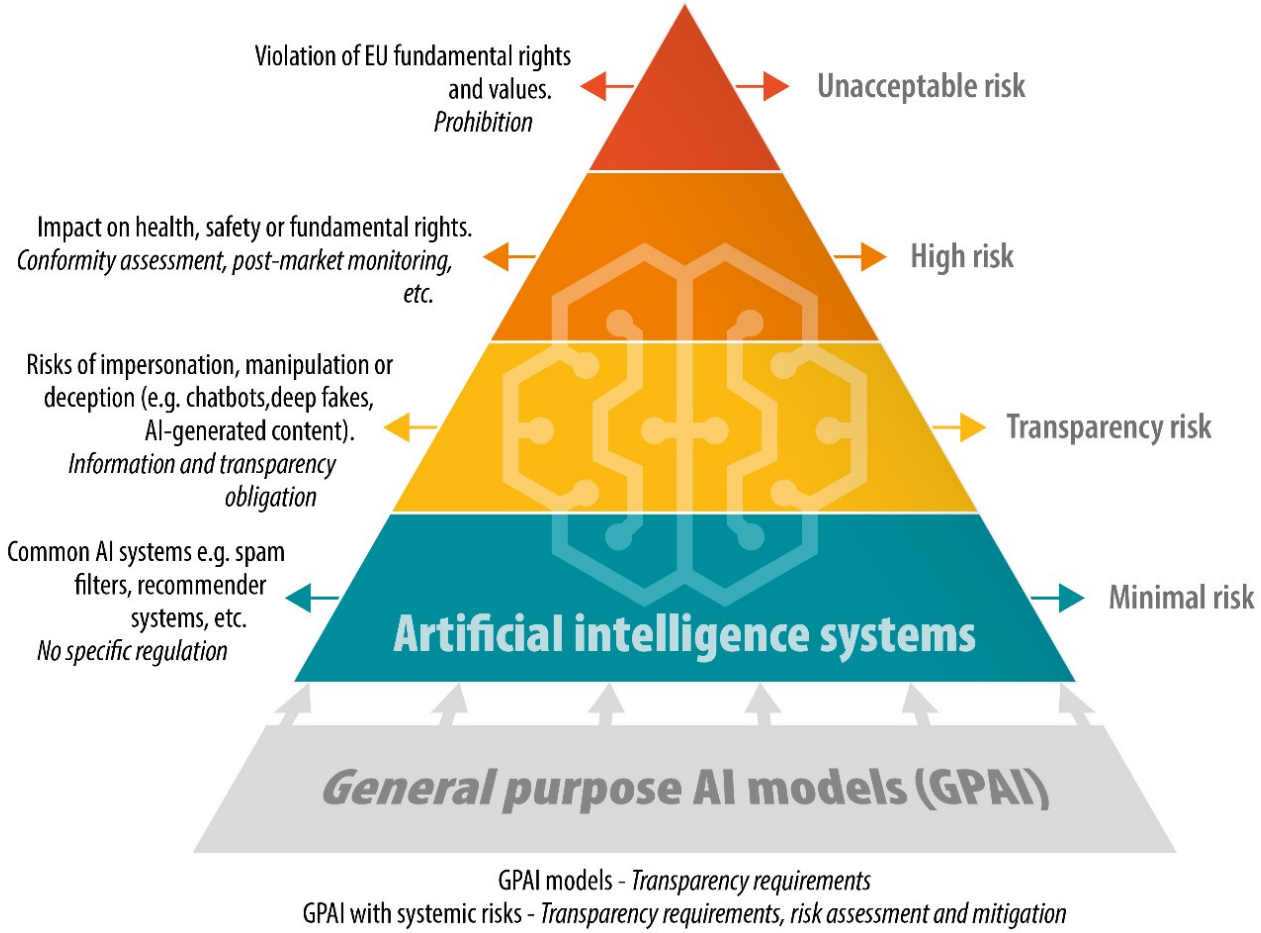
- ✓ **Fornitori** che immettono sul mercato o mettono in servizio sistemi di IA nell'UE, **indipendentemente da dove siano stabiliti**;
- ✓ **Deployer** che hanno sede o sono situati UE;
- ✓ **Fornitori** e **deployer** di sistemi di IA **situati in un paese terzo**, laddove l'**output** prodotto dal sistema è utilizzato in UE;
- ✓ **Importatori** e **distributori**;
- ✓ **Fabbricanti** che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto o con il loro nome o marchio;
- ✓ **Rappresentanti autorizzati** di fornitori non stabiliti nell'UE;
- ✓ **Persone interessate** che si trovano nell'UE.

NON si applica a:

- ✓ Settori che non rientrano nell'**ambito di applicazione del diritto dell'UE**;
- ✓ Sistemi di IA esclusivamente **per scopi militari, di difesa o sicurezza nazionale**;
- ✓ Sistemi di IA per **scopi di ricerca e sviluppo scientifico**;
- ✓ Attività di **ricerca, prova e sviluppo** relative a sistemi di IA;
- ✓ Deployer **persone fisiche che utilizzano sistemi di AI durante un'attività non professionale puramente personale**;
- ✓ Sistemi di IA rilasciati con **licenze free e open source** (salvo rischio).

PANETTA
Consulting Group

Risk-based approach



Considerando 26

Al fine di introdurre un **insieme proporzionato ed efficace** di regole vincolanti per i sistemi di IA è opportuno avvalersi di un **approccio basato sul rischio definito in modo chiaro**. Tale approccio dovrebbe **adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA**. È pertanto necessario **vietare** determinate pratiche di IA inaccettabili, **stabilire requisiti** per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché **obblighi di trasparenza** per determinati sistemi di IA.

PANETTA
Consulting Group

I sistemi ad alto rischio

Classificazione dei sistemi di IA come ad alto rischio

Sistemi usati come **componenti di sicurezza di un prodotto**, o che siano essi stessi un prodotto, sottoposti a una **disciplina di armonizzazione** di cui all'allegato I e, **al contempo**, che il prodotto o il sistema di IA è soggetto una **valutazione di conformità da parte di soggetti terzi** ai sensi della stessa normativa.

- Dispositivi medici
- Smart toys
- Ascensori
- ....

Sistemi di IA che rientrano tra quelli di cui all'**elenco** di previsto dall'allegato III.

- Biometria
- Infrastrutture critiche
- Istruzione e formazione professionale
- Occupazione, gestione dei lavoratori e accesso al lavoro autonomo
- Accesso e fruizione di prestazioni e servizi pubblici e di servizi privati essenziali
- Attività di contrasto
- Migrazione, asilo e controllo delle frontiere
- Amministrazione della giustizia e processi democratici

PANETTA
Consulting Group

Gli obblighi

Sistemi ad alto rischio

- *Sistema di gestione dei rischi*
- *Sorveglianza umana*
- *Documentazione tecnica*
- *Data governance*
- *Conservazione dei log*
- *Valutazione di impatto sui diritti fondamentali*
- *Sistema di gestione della qualità*
- *Accuratezza, robustezza e cybersicurezza*
- *Valutazione di conformità*
- *....*

Certi sistemi di IA

- *Obblighi di trasparenza*

Sistemi di IA per finalità generali

- *Documentazione tecnica*
- *Informazioni e documentazione ai provider*
- *Policy per rispettare le leggi UE sul diritto d'autore*
- *Report sui contenuti utilizzati per l'addestramento*
- *Obblighi ulteriori in caso di rischi sistemici*

AI ACT - ARTICOLO 15

*1. I **sistemi di IA ad alto rischio** sono progettati e sviluppati in modo tale da conseguire un **adeguato** livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita.*
2. Al fine di affrontare gli aspetti tecnici relativi alle modalità di misurazione degli adeguati livelli di accuratezza e robustezza di cui al paragrafo 1 e altre metriche di prestazione pertinenti, la Commissione, in cooperazione con i portatori di interessi e le organizzazioni pertinenti, quali le autorità di metrologia e di analisi comparativa, incoraggia, se del caso, lo sviluppo di parametri di riferimento e metodologie di misurazione.
3. I livelli di accuratezza e le pertinenti metriche di accuratezza dei sistemi di IA ad alto rischio sono dichiarati nelle istruzioni per l'uso che accompagnano il sistema.
*4. I sistemi di IA ad alto rischio sono **il più resilienti possibile** per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi. A tale riguardo sono adottate misure tecniche e organizzative.*
La robustezza dei sistemi di IA ad alto rischio può essere conseguita mediante soluzioni tecniche di ridondanza, che possono includere piani di backup o fail-safe.
*I sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio sono sviluppati in modo tale da eliminare o ridurre **il più possibile** il rischio di output potenzialmente distorti che influenzano gli input per operazioni future (feedback loops - "circuiti di feedback") e garantire che tali circuiti di feedback siano oggetto di adeguate misure di attenuazione.*
5. I sistemi di IA ad alto rischio sono resilienti ai tentativi di terzi non autorizzati di modificarne l'uso, gli output o le prestazioni sfruttando le vulnerabilità del sistema.
Le soluzioni tecniche volte a garantire la cibersicurezza dei sistemi di IA ad alto rischio sono adeguate alle circostanze e ai rischi pertinenti.
Le soluzioni tecniche finalizzate ad affrontare le vulnerabilità specifiche dell'IA includono, ove opportuno, misure volte a prevenire, accertare, rispondere, risolvere e controllare gli attacchi che cercano di manipolare il set di dati di addestramento (data poisoning - "avvelenamento dei dati") o i componenti preaddestrati utilizzati nell'addestramento (model poisoning - "avvelenamento dei modelli"), gli input progettati in modo da far sì che il modello di IA commetta un errore (adversarial examples - "esempi antagonistici", o model evasion, - "evasione dal modello"), gli attacchi alla riservatezza o i difetti del modello.

AI ACT - ARTICOLO 55

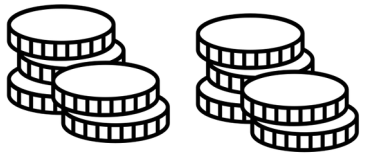
1. In aggiunta agli obblighi di cui agli articoli 53 e 54, i fornitori di modelli di IA per finalità generali con rischio sistemico:
a) effettuano una valutazione dei modelli in conformità di protocolli e strumenti standardizzati che rispecchino lo stato dell'arte, anche svolgendo e documentando il test contraddittorio (adversarial testing) del modello al fine di individuare e attenuare i rischi sistemici;
b) valutano e attenuano i possibili rischi sistemici a livello dell'Unione, comprese le loro fonti, che possono derivare dallo sviluppo, dall'immissione sul mercato o dall'uso di modelli di IA per finalità generali con rischio sistemico;
c) tengono traccia, documentano e riferiscono senza indebito ritardo all'ufficio per l'IA e, se del caso, alle autorità nazionali competenti, le informazioni pertinenti su incidenti gravi ed eventuali misure correttive per porvi rimedio;
*d) **garantiscono un livello adeguato di protezione della cibersicurezza per quanto riguarda il modello di IA per finalità generali con rischio sistemico e l'infrastruttura fisica del modello**.*
2. I fornitori di modelli di IA per finalità generali con rischio sistemico possono basarsi su codici di buone pratiche ai sensi dell'articolo 56 per dimostrare la conformità agli obblighi di cui al paragrafo 1 del presente articolo, fino alla pubblicazione di una norma armonizzata. La conformità alle norme armonizzate europee garantisce ai fornitori la presunzione di conformità nella misura in cui tali norme contemplano tali obblighi. I fornitori di modelli di IA per finalità generali con rischi sistemici che non aderiscono a un codice di buone pratiche approvato o che non si conformano alle norme armonizzate europee devono dimostrare mezzi alternativi adeguati di conformità ai fini della valutazione da parte della Commissione.
3. Le informazioni o la documentazione ottenute a norma del presente articolo, compresi i segreti commerciali, sono trattate in conformità degli obblighi di riservatezza di cui all'articolo 78.

PANETTA
Consulting Group

Sanzioni

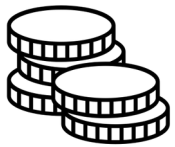
Fino a 35.000.000 di euro o, per le società, fino al 7% del fatturato mondiale totale annuo dell'esercizio precedente (se >)

Per violazioni relative a **pratiche di IA vietate**.



Fino a 15.000.000 di euro o, per le società, fino al 3% del fatturato mondiale totale annuo dell'esercizio precedente (se >)

Per la non conformità di un sistema di IA alle disposizioni connesse a **operatori** o organisti notificati, **diverse da quelle di cui all'articolo 5**.



Fino a 7.500.000 di euro o, per le società, fino al 1,5% del fatturato mondiale totale annuo dell'esercizio precedente (se >)

La **fornitura di informazioni inesatte, incomplete o fuorvianti** agli organismi notificati o alle autorità nazionali competenti per dare seguito a una richiesta.

PANETTA
Consulting Group

Timeline

Febbraio 2025

Diventano applicabili le norme sulle **pratiche di IA vietate**

Agosto 2025

Diventano applicabili gli obblighi per i **sistemi di IA per finalità generali**

Agosto 2026

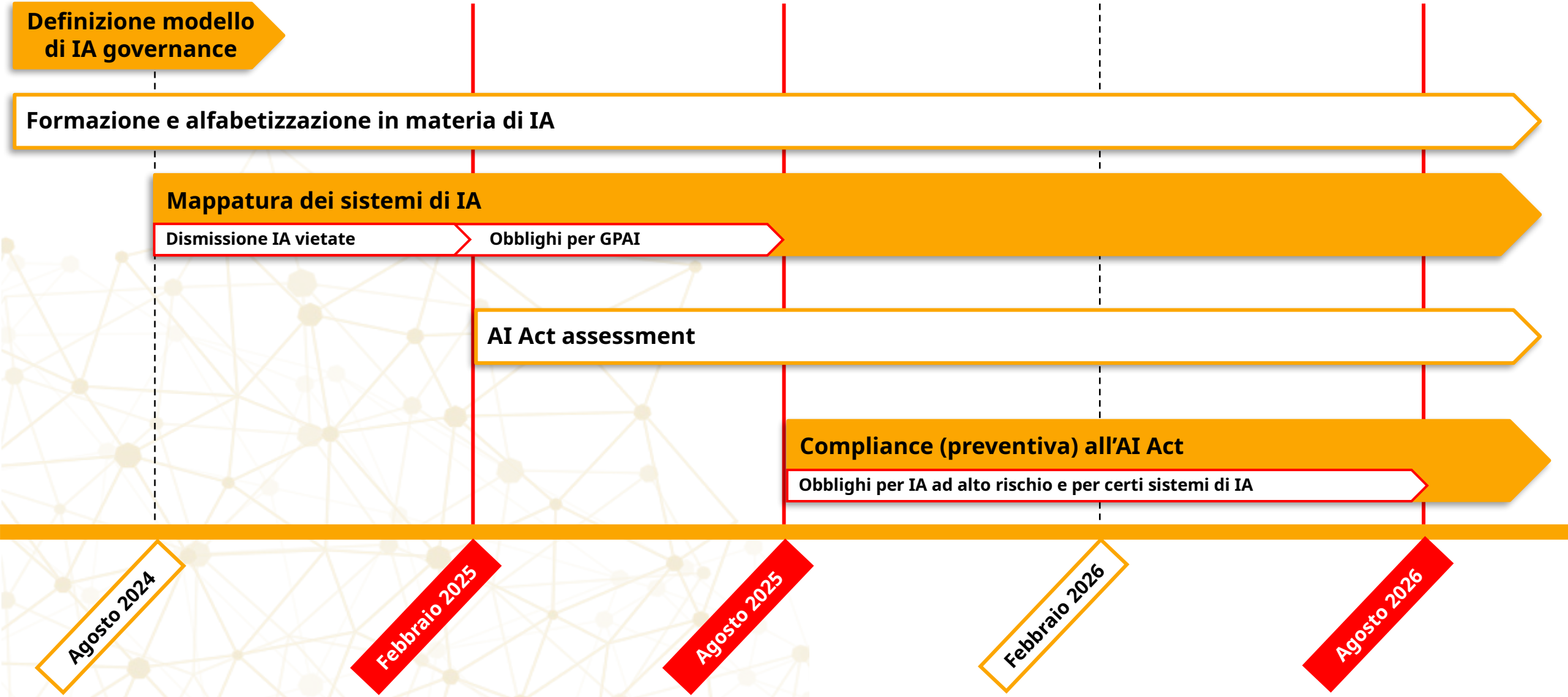
Diventano applicabili (quasi) **tutte le norme dell'AI Act**, compresi gli obblighi per i **sistemi ad alto rischio** definiti nell'allegato III

Agosto 2027

Diventano applicabili gli obblighi per i **sistemi ad alto rischio** definiti nell'allegato I (normativa di armonizzazione)

PANETTA
Consulting Group

Roadmap



PANETTA
Consulting Group

Alfabetizzazione

AI ACT - ARTICOLO 4

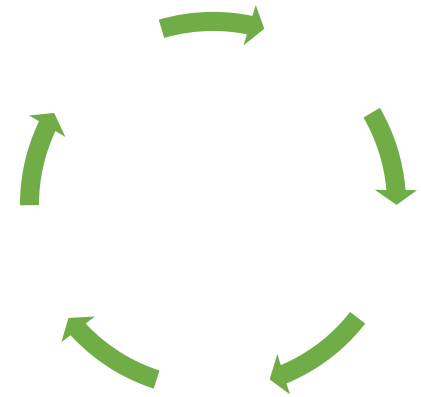
"*I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile* ***un livello sufficiente di alfabetizzazione in materia di IA del loro personale*** *nonché di* ***qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto****, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati*"

- *Mappatura preliminare dei sistemi di IA*
- *Definizione dei target (es. funzioni aziendali)*
- *Definizione di contenuti specifici e multidisciplinari*
- \+ *Policy interna sull'uso dei sistemi di IA*

PANETTA
Consulting Group

AI Act assessment

1	**Definizione di "sistema di IA"**	Verificare se il sistema considerato rientra nella definizione di "sistema di IA" prevista dall'AI Act.
2	**Campo di applicazione**	Verificare se le attività svolte dal sistema di IA o in connessione allo stesso rientrano nel campo di applicazione dell'AI Act o se opera un'eccezione.
3	**Determinazione del ruolo**	Verificare il ruolo ricoperto dalla Società/PA in relazione al sistema di IA considerato, inclusa la determinazione del ruolo di altre società del Gruppo e/o di eventuali fornitori e terze parti.
4	**Classificazione del rischio**	Determinare il livello di rischio relativamente al sistema di IA considerato, sulla base delle categorie e dei criteri di classificazione inclusi nell'AI Act, nonché dei successivi atti di implementazione ed esecuzione.
5	**Obblighi e requisiti applicabili**	Sulla base del livello di rischio identificato in relazione al sistema di IA considerato e al ruolo ricoperto dalla Società/PA ai sensi dell'AI Act, definire i requisiti, gli obblighi e gli adempimenti applicabili nel caso di specie.



PANETTA
Consulting Group

Grazie per l'attenzione

Avv. Gabriele Franco

SENIOR ASSOCIATE

g.franco@panetta.it

Piazza Colonna, 355
00187 - ROMA

panetta.it

PANETTA studio legale insAIde PRIVACY & TECHNOLOGY PROFESSIONALS strand alliance