Cyber & Cyber

Sicurezza • Dati • Geopolitica

AI ACT: OLTRE LA PIRAMIDE DEL RISCHIO

Come classificare i sistemi di intelligenza artificiale, individuare gli obblighi di fornitori e deployer e costruire una governance concreta

DI

Giuseppe Alverone



INDICE

IL RISCHIO NELL'AI ACT: LA PRIMA COSA DA CAPIRE È CHE NON ESISTE UN TERMOMETRO p.6

IL FORNITORE DAVANTI ALL'AI ACT: COME SI CLASSIFICA UN SISTEMA DI AI p.14

LA FINALITÀ PREVISTA DECIDE PIÙ DELL'ALGORITMO (MA NON LO CANCELLA) p.25

AI ACT: "AD ALTO RISCHIO" NON SIGNIFICA AVERE CALCOLATO UN RISCHIO ALTO p.32

QUANDO ARRIVA IL DEPLOYER: AI ACT, DPIA, FRIA E TRE VALUTAZIONI CHE NON DEVONO ESSERE CONFUSE p.39

DALLA TEORIA ALLA GOVERNANCE: LA SCHEDA DI CLASSIFICAZIONE AI ACT CHE OGNI ORGANIZZAZIONE DOVREBBE AVERE p.47



Giuseppe Alverone

Consulente, formatore e divulgatore in data protection, cybersecurity e gestione del rischio.
Lavora con un obiettivo preciso: portare le organizzazioni a prendere decisioni corrette nei momenti in cui ogni scelta ha conseguenze reali.
Generale di Brigata in congedo dell'**Arma dei Carabinieri**, ha prestato servizio per oltre **40 anni**, operando in contesti complessi dove decidere bene non è una scelta ma una necessità.
Questa esperienza oggi è il cuore del suo metodo: non parte dalla norma ma dalla realtà.
Non si limita a spiegare *GDPR* e *NIS 2*. Traduce obblighi in scelte operative e aiuta le organizzazioni a chiarire chi decide, su cosa e con quali responsabilità perché la sicurezza non nasce dai documenti ma da decisioni assunte e sostenute.
È stato **Data Protection Officer** dell'**Arma dei Carabinieri** fino al 2024.
Oggi è amministratore unico di **DATA FABER**, ricopre il ruolo di DPO a livello di gruppo in una primaria realtà industriale nazionale e affianca imprese e vertici aziendali che vogliono superare la compliance formale per costruire sistemi che funzionano davvero, integrando governance, processi e responsabilità.
È DPO certificato *UNI CEI EN 17740:2024*, docente presso **IF Academy**, presso **A-Sapiens Business School** e membro del **Comitato Scientifico A-SAPIENS**.
Autore di manuali e articoli specialistici, interviene in contesti di alto livello a diretto contatto con il top management.
Il suo metodo è diretto: leggere i segnali giusti, decidere con lucidità, tracciare ogni scelta.



Il rischio nell'AI Act

IL RISCHIO NELL'AI ACT: LA PRIMA COSA DA CAPIRE È CHE NON ESISTE UN TERMOMETRO

La rappresentazione dell'AI Act come una scala a quattro livelli di rischio è la stessa che la Commissione europea utilizza a fini divulgativi ed è coerente con l'"approccio basato sul rischio" enunciato nel considerando 26. Come indicatore funziona.
Diventa però fuorviante quando la si trasforma in una procedura operativa con cui il fornitore assegna al proprio sistema un'etichetta di rischio "minimo, limitato, alto o inaccettabile".
Il Regolamento non chiede al fornitore di scegliere un livello: costruisce regimi giuridici diversi, collegati a pratiche, finalità, casi d'uso e caratteristiche del sistema.
Comprendere questa differenza è il primo passo per classificare correttamente un sistema di AI e per non confondere la qualificazione normativa con la successiva gestione dei rischi.
Questo articolo dà conto anche di che cosa è cambiato con la versione consolidata del 27 luglio 2026.

La comoda immagine dei quattro livelli

Da quando si discute del *regolamento (UE) 2024/1689* (**AI Act**), una delle rappresentazioni più diffuse è quella della piramide dei rischi: rischio inaccettabile, rischio alto, rischio limitato e rischio minimo.
Va detto subito, per correttezza: non è un'invenzione dei divulgatori ma è lo schema con cui la stessa Commissione presenta il Regolamento, e il considerando 26 dichiara che il legislatore ha seguito un approccio basato sul rischio chiaramente definito, vietando determinate pratiche inaccettabili, stabilendo requisiti per i sistemi ad alto rischio e obblighi di trasparenza per determinati sistemi.
Come schema divulgativo, dunque, la piramide funziona e aiuta a trasmettere l'idea centrale del Regolamento secondo la quale gli obblighi crescono al crescere della rilevanza del rischio.
Il problema nasce quando questa immagine viene scambiata per la procedura giuridica prevista dal Regolamento.
In quel momento il fornitore rischia di porsi la domanda sbagliata: *"Quanto è rischioso il mio sistema e quale livello gli assegno?"*.
L'**AI Act** non gli affida un potere generale di graduazione del rischio ma gli chiede, prima di tutto, di verificare in quale disciplina ricade il sistema che intende immettere sul mercato o mettere in servizio.
Il bersaglio di questa esalogia non è la piramide, quindi, ma il suo uso come strumento di autovalutazione.
La differenza è sostanziale.

Una matrice di rischio produce normalmente un valore sulla base di probabilità e gravità.
Una qualificazione giuridica, invece, parte da fatti, finalità e caratteristiche del sistema e li confronta con fattispecie normative determinate.
Nell'**AI Act** le due operazioni esistono entrambe, ma non coincidono e, di regola, non avvengono nello stesso momento. Vedremo che il punto principale in cui, per il fornitore, le due operazioni si toccano è l'articolo 6, paragrafo 3, e che anche lì il Regolamento non lascia al fornitore una matrice libera.

La struttura reale dell'AI Act

L'**articolo 5** dell'**AI Act** disciplina le pratiche di AI vietate.
Qui non esiste un fornitore che calcola un punteggio e decide che il rischio è *"inaccettabile"*.
È il legislatore europeo che individua determinate pratiche e ne vieta l'immissione sul mercato, la messa in servizio o l'uso quando ricorrono le condizioni previste.
Dal **27 luglio 2026** l'elenco si è allungato di due voci, applicabili dal **2 dicembre 2026**: i sistemi che generano immagini intime realistiche di persone senza il loro consenso e quelli che generano o manipolano materiale pedopornografico.
Lo stesso Regolamento ne delimita la portata: per l'immissione sul mercato e la messa in servizio i divieti operano quando la generazione di quei contenuti è la finalità prevista del sistema, oppure è ragionevolmente prevedibile senza modifiche tecniche significative e mancano garanzie adeguate; per l'uso, quando il deployer impiega il sistema proprio a quello scopo.
L'articolo 6, invece, contiene le regole di classificazione dei sistemi di AI ad alto rischio (***high-risk***).
La norma individua due percorsi.
Il primo, al *paragrafo 1*, richiede due condizioni cumulative:
1. il sistema è destinato a essere usato come componente di sicurezza di un prodotto, oppure è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'Allegato I;
2. quel prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio.
Il secondo, al paragrafo 2, riguarda i sistemi che ricadono nei casi d'uso dell'Allegato III.
L'**articolo 50** dell'**AI Act** segue ancora una logica diversa.
Non crea una categoria generale denominata *"rischio limitato"* ma impone obblighi di trasparenza ai fornitori e ai deployer di determinati sistemi, in determinate circostanze: per esempio, quando un sistema è destinato a interagire direttamente con persone fisiche o genera contenuti sintetici.
Questi obblighi si sommano a quelli del **Capo III**, non li sostituiscono: lo dice espressamente il paragrafo 6 dello stesso articolo 50.
Un sistema ad alto rischio che interagisce con le persone è soggetto a entrambe le discipline.
Infine, la fascia che nel linguaggio divulgativo viene spesso chiamata *"rischio minimo"* non corrisponde a una categoria normativa autonoma dotata di un proprio articolo di classificazione.

È, in larga misura, l'area dei sistemi che non ricadono nei regimi più stringenti previsti dal Regolamento, per i quali l'**articolo 95** incoraggia codici di condotta volontari, ferme restando le altre norme eventualmente applicabili, a cominciare dall'obbligo di alfabetizzazione dell'articolo 4 dell'**AI Act** e dal **GDPR**.

Un'altra categoria: il rischio sistemico dei modelli per finalità generali

La semplificazione dei quattro livelli diventa ancora più evidente osservando il Capo V dell'AI Act.
L'**articolo 51** disciplina la classificazione dei modelli di AI per finalità generali (GPAI) con rischio sistemico.
Qui non stiamo semplicemente aggiungendo un quinto gradino alla piramide.
Il Regolamento guarda a un oggetto diverso che è il modello e non il sistema; e costruisce una disciplina specifica.
Un modello è classificato con rischio sistemico in due modi:
- **quando presenta capacità di impatto elevato, valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento. Si presume che un modello di AI per finalità generali abbia capacità di impatto elevato, quando la quantità cumulativa di calcolo utilizzata per il suo addestramento misurata in operazioni in virgola mobile è superiore a 10^{25}.**
- **oppure quando lo decide la Commissione – d'ufficio oppure a seguito di una segnalazione qualificata del gruppo di esperti scientifici – sulla base dei criteri dell'Allegato XIII.**

È un ulteriore motivo per evitare di ridurre tutto a una scala lineare.
L'**AI Act** è un sistema di qualificazioni e obblighi, non una tabella universale in cui ogni tecnologia deve essere collocata con un voto.

La parola decisiva è "classificazione"

Lo stesso titolo della sezione 1 del Capo III è indicativo: *"Classificazione dei sistemi di IA come ad alto rischio"*. L'articolo 6 parla di regole di classificazione.
Questo linguaggio non è casuale.
Il fornitore deve ricostruire la fattispecie.
Deve comprendere:
- **che cosa ha sviluppato;**
- **a quale uso lo destina;**
- **in quale contesto dovrà essere impiegato e se quelle caratteristiche fanno scattare una delle disposizioni del Regolamento.**

Solo successivamente, quando il sistema è qualificato come ad alto rischio, entra in gioco in modo pieno il sistema di gestione dei rischi dell'articolo 9.
Qui l'**AI Act** utilizza il rischio nel senso tecnico definito dall'articolo 3, punto 2: la combinazione della probabilità del verificarsi di un danno e della gravità del danno stesso.

È quindi essenziale mantenere separate due domande.
La prima è: *"Questo sistema è giuridicamente un sistema di AI ad alto rischio ai sensi dell'articolo 6?"*.
La seconda è: *"Quali rischi concreti presenta e come devono essere identificati, stimati, valutati e trattati?"*.
La prima riguarda la classificazione. La seconda riguarda il risk management.

Il punto di contatto: l'articolo 6, paragrafo 3 dell'AI Act

Sarebbe scorretto tacere che, in un caso, un giudizio sul rischio entra dentro la classificazione.
L'articolo 6, paragrafo 3, consente di non considerare ad alto rischio un sistema dell'Allegato III che *"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"*, purché:
- **ricorra una delle quattro condizioni tipizzate dalla norma;**
- **e il sistema non effettui profilazione di persone fisiche.**

Ma anche qui non c'è un termometro. C'è:
- **una soglia normativa ("rischio significativo");**
- **un elenco chiuso di condizioni;**
- **una preclusione assoluta (la profilazione, che rende il sistema sempre ad alto rischio);**
- **un obbligo di documentazione e di registrazione (paragrafo 4 e articolo 49, paragrafo 2);**
- **un controllo successivo dell'autorità di vigilanza del mercato, che può riqualificare il sistema e, in caso di classificazione elusiva, applicare le sanzioni dell'articolo 99 (articolo 80).**

Ne parleremo nell'articolo 4 di questa esalogia. Per ora basta fissare il principio: l'eccezione è un'autovalutazione vincolata e controllabile, non una libera autocertificazione.

Il rischio di una cattiva semplificazione

La confusione tra classificazione e valutazione produce conseguenze pratiche.
Un fornitore potrebbe ritenere erroneamente che un sistema non sia ad alto rischio perché una propria matrice interna restituisce un rischio moderato; oppure potrebbe qualificare come ad alto rischio un sistema soltanto perché attribuisce un valore elevato alla gravità di un possibile danno, senza verificare se ricorra la fattispecie dell'articolo 6.
Entrambi gli approcci sono sbagliati.
La classificazione deriva dalle regole dell'AI Act.
Il risk assessment serve poi a governare i rischi del sistema nei casi e con le modalità previste dalla disciplina applicabile.
Anche le linee guida della Commissione sulla classificazione dei sistemi ad alto rischio, previste dall'articolo 6, paragrafo 5, e pubblicate in bozza il 19 maggio 2026 (**con consultazione chiusa il 23 luglio 2026 e versione definitiva attesa entro la fine dell'anno**), seguono questa impostazione.

Sono costruite attorno all'articolo 6 e ai due percorsi dell'Allegato I e dell'Allegato III, con esempi di sistemi che sono e che non sono ad alto rischio.
Non propongono una matrice universale con cui assegnare a ogni sistema uno dei quattro colori della piramide.

Che cosa è cambiato il 27 luglio 2026

Questa serie di sei articoli è aggiornata alla versione consolidata del *Regolamento (UE) 2024/1689* del 27 luglio 2026.
Quella data non è casuale: è il giorno in cui è entrato in vigore il *Regolamento (UE) 2026/1744* dell'8 luglio 2026, pubblicato nella **Gazzetta ufficiale dell'Unione europea** il 24 luglio 2026 e noto come **Digital Omnibus on AI**.
È utile riassumere che cosa è cambiato, perché diverse modifiche toccano proprio la classificazione.
Innanzitutto il calendario. Gli obblighi per i sistemi ad alto rischio dell'Allegato III si applicano dal **2 dicembre 2027** e quelli per i sistemi dell'**Allegato I dal 2 agosto 2028**, con date fisse.
Gli obblighi di trasparenza dell'articolo 50 restano applicabili dal 2 agosto 2026, con una sola proroga: la marcatura leggibile meccanicamente dei contenuti sintetici prevista dal paragrafo 2, per i sistemi già immessi sul mercato prima del 2 agosto 2026, è dovuta dal 2 dicembre 2026.
I due nuovi divieti dell'articolo 5 si applicano dal **2 dicembre 2026**.
Poi l'articolo 6 ha acquisito, dopo il paragrafo 1, tre nuovi paragrafi: 1 bis, 1 ter e 1 quater.
Il loro scopo è delimitare la nozione di componente di sicurezza e la seconda condizione del paragrafo 1.
Il primo chiarimento riguarda la funzione del sistema.
Non è un componente di sicurezza il sistema di AI usato soltanto per scopi che non riguardano la sicurezza: assistere l'utente, ottimizzare le prestazioni, rendere più efficiente il servizio, automatizzare, aumentare la comodità o controllare la qualità.
La regola ha però un'eccezione. Se il guasto o il malfunzionamento di quel sistema mette in pericolo la salute o la sicurezza delle persone, il sistema torna a essere un componente di sicurezza.
Il secondo chiarimento riguarda la valutazione della conformità.
Alcuni prodotti sono sottoposti a valutazione di terza parte solo per rischi che non toccano la salute o la sicurezza, per esempio la distribuzione dello spettro radio o le interferenze elettromagnetiche.
In questi casi la seconda condizione del paragrafo 1 dell'articolo 6 non è soddisfatta.
Il sistema, per questa via, non è ad alto rischio.
C'è infine una modifica all'Allegato I. Il regolamento macchine è passato dalla sezione A alla sezione B.

Per i sistemi di AI integrati nelle macchine si applica quindi il regime speciale dell'articolo 2, paragrafo 2, di cui parleremo nel prossimo articolo della nostra esalogia.
Ancora:
- **l'articolo 4 sull'alfabetizzazione in materia di AI richiede ora a fornitori e deployer di adottare misure a sostegno dello sviluppo dell'alfabetizzazione del personale, senza dover garantire un livello determinato a ciascuna persona;**
- **la registrazione nella banca dati dell'Unione dei sistemi che il fornitore ritiene non ad alto rischio ai sensi dell'articolo 6, paragrafo 3, è stata mantenuta, ma con informazioni semplificate;**
- **con il nuovo articolo 4 bis, la facoltà di trattare categorie particolari di dati per individuare e correggere le distorsioni, prevista dall'articolo 10, paragrafo 5, è stata estesa a tutti i sistemi di AI, nei limiti della stretta necessità e con garanzie, senza trasformarsi in un obbligo;**
- **il nuovo paragrafo 13 dell'articolo 2 consente alla Commissione, con atti delegati da adottare entro il 2 agosto 2027, di limitare alcuni requisiti del Capo III per i sistemi collegati a prodotti della sezione A dell'Allegato I, quando la normativa di prodotto assicura un livello di protezione equivalente o superiore;**
- **l'articolo 27, paragrafo 4, consente ora al deployer di rinviare, nella valutazione d'impatto sui diritti fondamentali, alle sezioni pertinenti della DPIA o di riprenderne le parti rilevanti.**

Tre novità riguardano infine chi è agevolato, chi vigila e chi è già sul mercato.
Le piccole imprese a media capitalizzazione entrano nel regime di favore finora riservato alle PMI.
La definizione è nel nuovo punto 14 ter dell'articolo 3. Tra le agevolazioni principali:
- **documentazione tecnica semplificata (articolo 11, paragrafo 1);**
- **sistema di gestione della qualità proporzionato (articolo 17, paragrafo 2);**
- **accesso prioritario allo spazio di sperimentazione dell'Unione (articolo 57, paragrafo 3 bis);**
- **tetto alle sanzioni (articolo 99, paragrafo 6 bis).**

L'Ufficio per l'IA acquisisce una competenza esclusiva di vigilanza (articolo 75, paragrafo 1). Riguarda due categorie di sistemi:
- **quelli basati su un modello per finalità generali, quando modello e sistema sono sviluppati dallo stesso fornitore o da fornitori della stessa impresa;**
- **quelli integrati nelle piattaforme online e nei motori di ricerca di dimensioni molto grandi. I poteri di indagine, ispezione e sanzione sono nei nuovi articoli da 75 bis a 75 quinquies.**

I sistemi ad alto rischio già sul mercato restano fuori dal regime finché la loro progettazione non cambia in modo significativo (***articolo 111, paragrafo 2, riscritto***).
Fanno eccezione i sistemi destinati a essere usati da autorità pubbliche: fornitori e deployer devono comunque renderli conformi entro il **2 agosto 2030**.
Nulla di tutto questo modifica la logica della classificazione.
Ne modifica però i confini (l'Allegato I) e il tempo (le date di applicazione), e un fornitore che classifica oggi deve tenerne conto.

Conclusioni

In conclusione, quando si parla di rischio nell'AI Act, il primo errore da evitare è linguistico e metodologico insieme.
Non dobbiamo chiedere al fornitore di *"scegliere il livello di rischio"*; dobbiamo, invece, chiedergli di qualificare correttamente il sistema ai sensi dell'AI Act e di documentare il percorso che lo ha portato a quella conclusione.
Quindi, prima si qualifica il sistema, poi, dove richiesto, si valutano e si gestiscono i rischi concreti.
Nel prossimo articolo entreremo nel cuore operativo del problema: vedremo, passo dopo passo, come un fornitore può classificare davvero un sistema di IA, quali domande deve porsi e in quale ordine.

Articolo del 9 ottobre 2026



Il fornitore davanti all’AI Act

IL FORNITORE DAVANTI ALL'AI ACT: COME SI CLASSIFICA UN SISTEMA DI AI

Nessuna autorità attribuisce preventivamente a un fornitore la qualificazione del proprio sistema: spetta allo stesso fornitore applicare l'AI Act, motivare la classificazione adottata e dimostrare il percorso seguito, fermo restando che quella valutazione potrà essere verificata successivamente dalle autorità competenti.
Questo articolo ricostruisce il percorso decisionale corretto, nell'ordine previsto dal Regolamento: verificare se l'AI Act si applica, accertare se si è davanti a un sistema di AI, individuarne la finalità prevista, escludere le pratiche vietate, stabilire se il sistema è ad alto rischio e con quali eccezioni, identificare gli obblighi di trasparenza e capire da quando tutto questo diventa operativo.
La tesi di fondo è che la classificazione non sia una scelta discrezionale del fornitore ma una conclusione alla quale si arriva applicando le regole con rigore, lungo un percorso che deve poter essere spiegato, documentato e, ove richiesto, registrato.

La domanda sbagliata

Immaginiamo una riunione per la realizzazione di un prodotto.
Il team ha sviluppato un assistente AI che legge documenti, estrae informazioni e propone una decisione a chi lo usa.
A un certo punto qualcuno chiede: *"Per l'AI Act siamo a basso rischio, giusto?".*
È la domanda più naturale del mondo ed è la domanda sbagliata.
L'AI Act non chiede al fornitore quanto sia rischioso il suo sistema; gli chiede in quale disciplina ricada.
La differenza sembra sottile e invece cambia completamente il contesto: alla prima domanda si risponde con un'opinione, alla seconda con un ragionamento giuridico che deve reggere davanti a chi lo verificherà.
Questo articolo racconta quel ragionamento, una domanda alla volta.

Nessuno classifica al posto del fornitore (ma qualcuno controlla)

Nel modello dell'AI Act non esiste, come regola generale, un'autorità che esamina in anticipo ogni sistema e gli assegna una categoria.
La qualificazione iniziale spetta a chi sviluppa o fa sviluppare il sistema e lo immette sul mercato o lo mette in servizio con il proprio nome o marchio: il fornitore, secondo la definizione dell'articolo 3, punto 3 dell'AI Act.
Questo non significa che il fornitore sia lasciato solo con la propria opinione.
I controlli esistono, ma arrivano dopo, e ciascuno a suo modo.

N.1 La valutazione della conformità

Per i sistemi dell'Allegato I, e a certe condizioni per i sistemi biometrici dell'Allegato III, passa da un organismo notificato (**articolo 43 AI Act**); per gli altri sistemi dell'Allegato III avviene con il controllo interno.
In ogni caso si conclude con la dichiarazione UE di conformità e con la marcatura CE, che il fornitore appone (**articoli 47 e 48 AI Act**).
La marcatura esiste, ma è il punto d'arrivo di un percorso, non il suo inizio, e presuppone una classificazione già fatta.

N.2 Trasparenza

I sistemi ad alto rischio dell'Allegato III, con l'eccezione delle infrastrutture critiche registrate a livello nazionale, e i sistemi che il fornitore ha ritenuto esenti finiscono nella banca dati dell'Unione (**articolo 49 AI Act**).
La qualificazione, in altre parole, lascia una traccia conoscibile, in larga parte accessibile al pubblico; fanno eccezione i sistemi per le attività di contrasto, la migrazione, l'asilo e il controllo delle frontiere, registrati in una sezione sicura non pubblica (**articolo 49, paragrafo 4**).

N.3 Questo è ciò che pesa di più

L'autorità di vigilanza del mercato conserva i poteri generali previsti dall'**articolo 74 AI Act** e dal *Regolamento (UE) 2019/1020* e, per i sistemi che il fornitore ha ritenuto esenti ai sensi dell'articolo 6, paragrafo 3, dispone di una procedura dedicata: può valutarli, imporne la messa in conformità e, se la classificazione è servita a eludere i requisiti, applicare le sanzioni dell'articolo 99 (**articolo 80 AI Act**).
Il punto, quindi, è l'ordine secondo il quale:

- **prima il fornitore qualifica;**
- **poi organismi notificati, banca dati e autorità verificano.**

La marcatura CE arriva dopo la qualificazione, non al posto di essa, e il fornitore non è libero di decidere come preferisce.

Deve applicare un insieme di norme che delimitano la sua valutazione e deve saper dimostrare perché ha concluso che il sistema ricade, oppure non ricade, in uno specifico regime.
L'operazione assomiglia alla qualificazione giuridica di un fatto, non alla compilazione di una matrice; quindi:
- **prima si ricostruisce il fatto;**
- **poi si individua la norma;**
- **infine si verifica se gli elementi del fatto corrispondono alla fattispecie.**

Domanda zero: l'AI Act si applica?

C'è una domanda che viene quasi sempre saltata, perché sembra ovvia: l'AI Act si applica a questo sistema, a questo soggetto, a questo uso?
La risposta sta nell'articolo 2, e non è sempre sì.
L'ambito territoriale (**paragrafo 1**) è ampio: copre i fornitori che immettono sul mercato o mettono in servizio sistemi nell'Unione, ovunque siano stabiliti; i deployer stabiliti nell'Unione; e, in determinati casi, i fornitori e i deployer di paesi terzi il cui output è utilizzato nell'Unione.
Le esclusioni contano altrettanto. Il Regolamento non si applica:
- **ai sistemi immessi sul mercato, messi in servizio o utilizzati esclusivamente per scopi militari, di difesa o di sicurezza nazionale (paragrafo 3);**
- **alle autorità pubbliche di paesi terzi e alle organizzazioni internazionali, nell'ambito della cooperazione internazionale di polizia e giudiziaria, purché vi siano garanzie adeguate (paragrafo 4);**
- **ai sistemi sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici (paragrafo 6);**
- **alle attività di ricerca, prova e sviluppo che precedono l'immissione sul mercato, salvo le prove in condizioni reali (paragrafo 8);**
- **ai deployer persone fisiche che usano i sistemi per attività personali non professionali (paragrafo 10);**
- **ai sistemi rilasciati con licenza libera e open source, a meno che non siano immessi sul mercato come sistemi ad alto rischio, vietati o soggetti all'articolo 50 (paragrafo 12).**

C'è infine un regime speciale, previsto dal paragrafo 2, che riguarda i prodotti della sezione B dell'Allegato I.
Lo spiegheremo tra poco, quando arriveremo all'articolo 6: qui basti dire che un fornitore che classifica un sistema destinato a un veicolo o a un aeromobile deve saperlo prima di compilare qualsiasi scheda.

Prima domanda: è davvero un sistema di AI?

Il percorso entra nel vivo con l'articolo 3, punto 1 dell'AI Act.
Il Regolamento definisce il sistema di AI attraverso una serie di elementi: un sistema automatizzato, con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dagli input come generare output quali previsioni, contenuti, raccomandazioni o decisioni capaci di influenzare ambienti fisici o virtuali.
La verifica non è una formalità.
Le linee guida della Commissione sulla definizione di sistema di AI, pubblicate il **6 febbraio 2025**, indicano nella capacità di inferenza l'elemento che distingue un sistema di AI dal software tradizionale, quello che segue regole scritte interamente da persone.
Se una soluzione non rientra nella definizione, il percorso di classificazione si ferma qui.
Se invece vi rientra, chiamarla *"software tradizionale"* non la sottrae al Regolamento.
Il fornitore dovrebbe quindi documentare, in poche righe, perché considera la soluzione dentro o fuori la definizione.
Questa è già governance; non serve una relazione di cinquanta pagine: serve una motivazione intelligibile e verificabile.

Seconda domanda: qual è la finalità prevista?

Subito dopo viene la finalità prevista (*intended purpose*), uno dei concetti più importanti dell'intero **AI Act**, perché collega tecnologia, funzione e contesto d'uso.
L'**articolo 3, punto 12**, la definisce come l'uso a cui il fornitore destina il sistema, compresi il contesto e le condizioni d'uso specifici, come indicato nelle istruzioni per l'uso, nel materiale promozionale o di vendita, nelle dichiarazioni e nella documentazione tecnica.
Il fornitore deve quindi dire che cosa il sistema è destinato a fare, per chi, in quale processo e in quali condizioni.
Quindi l'espressione *"Strumento di supporto decisionale"* non basta: una descrizione così ampia impedisce qualsiasi classificazione affidabile.
Un sistema che corregge testi e un sistema che filtra candidature possono condividere la stessa tecnologia, ma la loro finalità prevista li porta in mondi normativi diversi e poiché la definizione include espressamente il materiale promozionale, chi vende il prodotto come strumento per selezionare candidati non può poi sostenerne una finalità neutra e generica per tenersi fuori dall'Allegato III.

Terza domanda: l'uso è vietato?

Prima ancora di ragionare sull'alto rischio, il fornitore deve verificare che l'immissione sul mercato, la messa in servizio o l'uso previsto non ricadano in una pratica vietata dall'articolo 5, letto insieme alle linee guida della Commissione sulle pratiche vietate del **4 febbraio 2025**.
Qui il ragionamento è binario.
Se ricorrono gli elementi della fattispecie, non si sale a una categoria *"più alta"*: quella pratica, nelle condizioni indicate dal Regolamento, semplicemente non può essere svolta.
Alcuni divieti guardano all'uso più che alla tecnologia.
Il riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione, per esempio, è vietato salvo motivi medici o di sicurezza (*paragrafo 1, lettera f*).
Le linee guida della Commissione sulle pratiche vietate leggono la nozione di luogo di lavoro in modo da comprendere anche i candidati nei processi di selezione al paragrafo 253: chi progetta uno strumento per i colloqui di selezione deve saperlo prima di aprire l'Allegato III.
Dal **2 dicembre 2026**, inoltre, l'elenco comprende i due nuovi divieti introdotti dal *Regolamento (UE) 2026/1744*, sui contenuti intimi non consensuali e sul materiale pedopornografico, nei limiti che lo stesso Regolamento fissa.
Questa verifica precede ogni tentativo di rappresentare il sistema come *"alto"*, *"medio"* o *"basso"* rischio.

Quarta domanda: è ad alto rischio? Il percorso dei prodotti

A questo punto si entra nella classificazione vera e propria, e l'articolo 6 offre due percorsi.
Il primo, al paragrafo 1, riguarda i sistemi legati ai prodotti e richiede due condizioni cumulative:

- **il sistema è componente di sicurezza di un prodotto disciplinato dalla normativa di armonizzazione elencata nell'Allegato I, oppure è esso stesso quel prodotto;**
- **il prodotto è soggetto a una valutazione della conformità da parte di terzi.**

Dal **27 luglio 2026** la norma è ancor più precisa.
Non è componente di sicurezza il sistema usato soltanto per assistere l'utente, ottimizzare le prestazioni, rendere più efficiente il servizio, automatizzare, aumentare la comodità o controllare la qualità, a meno che un suo malfunzionamento metta in pericolo la salute o la sicurezza delle persone.
Quindi, una valutazione di terza parte imposta soltanto per rischi diversi da quelli per la salute e la sicurezza, come le interferenze radio, non basta a soddisfare la seconda condizione.
Qui serve una piccola mappa, perché il Regolamento usa etichette che non spiegano se stesse.
Il *"Capo III"* è la parte dell'**AI Act** dedicata ai sistemi ad alto rischio: contiene le regole di classificazione, i requisiti che il sistema deve rispettare (gestione dei rischi, dati, documentazione, sorveglianza umana, accuratezza), gli obblighi del fornitore e la valutazione della conformità; è, in sostanza, il regime dell'alto rischio.

L'*"Allegato I"* è l'elenco delle normative europee di prodotto con cui l'**AI Act** si intreccia e ha due sezioni.
La sezione A raccoglie le normative costruite sul modello armonizzato europeo: giocattoli, ascensori, apparecchiature radio, dispositivi medici e altri prodotti che portano la marcatura CE.
Per un sistema di AI che è componente di sicurezza di uno di questi prodotti il Capo III si applica direttamente: i requisiti dell'**AI Act** si aggiungono a quelli della normativa di prodotto e vengono verificati insieme, in un'unica valutazione della conformità.
Il *Regolamento (UE) 2026/1744* ha però previsto che la Commissione, con atti delegati da adottare entro il **2 agosto 2027**, possa limitare alcuni requisiti del Capo III quando la normativa di prodotto assicura già un livello di protezione equivalente o superiore (articolo 2, paragrafo 13).
La sezione B raccoglie invece settori che hanno un proprio sistema di omologazione, molto strutturato e con proprie autorità: **veicoli, aviazione civile, ferrovie, equipaggiamento marittimo** e, dal **27 luglio 2026**, macchine.
Per questi prodotti l'AI Act non impone i requisiti del Capo III in modo diretto ma prevede che siano le rispettive normative di settore a incorporarli, nei tempi e nei modi che quei settori decideranno.
Nel frattempo, dell'**AI Act** si applicano soltanto la regola di classificazione dell'articolo 6, paragrafo 1, l'articolo 60 bis e gli articoli da 102 a 112, tra i quali le disposizioni che modificano proprio quelle normative di settore.
Questo è il regime speciale dell'articolo 2, paragrafo 2.
In pratica: il fornitore di un sistema di AI per un'automobile classifica il sistema con l'AI Act, ma i requisiti da rispettare li troverà nelle regole di omologazione dei veicoli.

Quarta domanda, seconda parte: il percorso dei casi d'uso

Il secondo percorso è più semplice da raccontare.
L'articolo 6, paragrafo 2, dice che sono ad alto rischio i sistemi elencati nell'Allegato III.
Qui non contano i prodotti, ma i campi in cui il sistema viene usato.
Il legislatore ha individuato otto aree in cui un sistema di AI può incidere sui diritti delle persone e ha elencato, per ciascuna, i casi d'uso che considera ad alto rischio:
- **la biometria;**
- **le infrastrutture critiche;**
- **l'istruzione e la formazione professionale;**
- **l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo;**
- **l'accesso ai servizi privati essenziali e alle prestazioni e ai servizi pubblici essenziali;**
- **le attività di contrasto;**
- **la migrazione, l'asilo e il controllo delle frontiere;**
- **l'amministrazione della giustizia e i processi democratici.**

Il fornitore confronta la finalità prevista del suo sistema con questi casi d'uso.
Non deve cercare *"altri casi"*, perché non esistono: l'elenco è chiuso.

Al di fuori di una modifica legislativa, può aggiornarlo soltanto la Commissione con atti delegati (articolo 7), aggiungendo o modificando casi d'uso all'interno delle otto aree, oppure sopprimendone.

L'eccezione e il suo limite

Se il sistema ricade nell'Allegato III, resta una possibilità prevista dall'articolo 6, paragrafo 3.
La norma consente di non considerare ad alto rischio un sistema che 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"*, quando ricorre almeno una delle seguenti condizioni che si profilano quando il sistema è destinato a:

- **eseguire un compito procedurale limitato;**
- **migliorare il risultato di un'attività umana precedentemente completata;**
- **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;**
- **eseguire un compito preparatorio per una valutazione pertinente ai casi d'uso dell'Allegato III.**

C'è però un limite che chiude la porta prima ancora di aprirla: un sistema dell'Allegato III è sempre considerato ad alto rischio se effettua profilazione di persone fisiche, nel senso dell'**articolo 4, punto 4, del GDPR richiamato dall'articolo 3, punto 52**.
Pertanto, chi valuta aspetti personali di una persona, chi ne prevede il rendimento professionale, l'affidabilità o il comportamento, non può invocare la deroga, qualunque sia la sua opinione sul rischio; e chi la invoca legittimamente non ha finito perché l'articolo 6, paragrafo 4, gli richiede di documentare la valutazione prima dell'immissione sul mercato o della messa in servizio, di registrare il sistema nella banca dati dell'Unione ai sensi dell'articolo 49, paragrafo 2 **(obbligo confermato, con contenuti semplificati, dal Regolamento (UE) 2026/1744)** e di consegnare la documentazione alle autorità che la richiedano.
L'articolo 80 chiude il cerchio: se l'autorità di vigilanza ha motivo di ritenere che il sistema sia in realtà ad alto rischio, lo valuta, può imporre la messa in conformità entro un termine e, quando la classificazione è servita a eludere i requisiti, applica le sanzioni dell'articolo 99.
Le linee guida della Commissione europea sulla classificazione previste dall'articolo 6, paragrafo 5, pubblicate in bozza il **19 maggio 2026**, aiutano a leggere le quattro condizioni e portano esempi per ciascuna area dell'Allegato III.
Non sono vincolanti, e sono ancora una bozza; ma chi se ne discosta farà bene a saper spiegare perché, perché sarà la prima domanda di un'autorità di vigilanza.

Quinta domanda: si applica l'articolo 50?

La classificazione non finisce con l'articolo 6.
Il fornitore deve verificare anche se il sistema rientri negli "obblighi di trasparenza per i fornitori e i deployer di determinati sistemi di IA": è il titolo esatto dell'articolo 50, e dice già che gli obblighi sono di due tipi.
Sul fornitore ne gravano due:

- **i sistemi destinati a interagire direttamente con persone fisiche devono essere progettati in modo che le persone sappiano di interagire con un sistema di AI, a meno che ciò non sia evidente (paragrafo 1);**
- **i sistemi che generano audio, immagini, video o testo sintetici devono marcare gli output in un formato leggibile meccanicamente, in modo che siano rilevabili come generati o manipolati artificialmente (paragrafo 2); l'obbligo non si applica nella misura in cui i sistemi svolgono una funzione di assistenza per l'editing standard, come la correzione grammaticale, o non modificano in modo sostanziale i dati di input forniti dal deployer.**

Sul deployer gravano altri obblighi: **informare le persone esposte a sistemi di riconoscimento delle emozioni o di categorizzazione biometrica** (*paragrafo 3*) **e rendere noto che un contenuto è un deep fake, o che un testo pubblicato su questioni di interesse pubblico è stato generato artificialmente** (*paragrafo 4*).
Il fornitore deve conoscerli, perché le sue istruzioni per l'uso devono mettere il deployer in condizione di rispettarli.
Tre precisazioni.
Gli obblighi dell'articolo 50 si sommano a quelli del Capo III (paragrafo 6).
Si applicano dal **2 agosto 2026**, con la sola proroga al 2 dicembre 2026 per la marcatura dei sistemi già sul mercato e sono oggi accompagnati da due strumenti:

- **le linee guida definitive della Commissione sull'articolo 50, adottate il 20 luglio 2026;**
- **il Codice di buone pratiche sulla trasparenza dei contenuti generati dall'AI, pubblicato nella versione finale il 10 giugno 2026 e valutato adeguato dalla Commissione e dal Consiglio per l'IA.**

Anche qui è più corretto parlare di *"sistema soggetto agli obblighi dell'articolo 50"* che di "sistema a rischio limitato".
La seconda formula è comoda mentre la prima è giuridicamente precisa.

Sesta domanda: c'è di mezzo un modello per finalità generali?

Il Capo V si rivolge ai fornitori di modelli di AI per finalità generali, non ai fornitori di sistemi.
Chi integra nel proprio sistema un modello sviluppato da altri è un *"fornitore a valle"*: riceve dal fornitore del modello le informazioni e la documentazione previste dall'articolo 53, paragrafo 1, lettera b), e le usa per la propria conformità.
Diventa a sua volta fornitore del modello soltanto se lo modifica in modo significativo, secondo i criteri delle linee guida della Commissione sui modelli per finalità generali del 18 luglio 2025.
Due punti però toccano da vicino la classificazione del sistema.
Il primo: un sistema basato su un modello per finalità generali e capace di servire a varie finalità è un *"sistema di AI per finalità generali"* (**articolo 3, punto 66**), e le linee guida in bozza sull'alto rischio presumono che la sua finalità prevista comprenda gli usi dell'Allegato III, quando questi sono fattibili e ragionevolmente prevedibili date le sue capacità, a meno che il fornitore li escluda in modo chiaro e coerente in tutta la documentazione.
Il secondo: l'articolo 25, paragrafo 1, lettera c), menziona espressamente i sistemi per finalità generali tra quelli la cui modifica di finalità da parte di un terzo può far nascere un nuovo fornitore.
Le due regole vanno lette insieme: se il fornitore non ha escluso gli usi ad alto rischio, quegli usi rientrano nella sua finalità prevista e gli obblighi restano suoi; se li ha esclusi in modo chiaro e coerente, chi impiega comunque il sistema per un uso dell'Allegato III ne diventa fornitore.
Ne parleremo nel prossimo articolo.

Settima domanda: da quando?

L'ultimo passaggio colloca la qualificazione nel tempo.
Dopo il *Regolamento (UE) 2026/1744* il calendario è questo:
- **i divieti dell'articolo 5 si applicano già, e i due nuovi si applicano dal 2 dicembre 2026;**
- **l'articolo 50 si applica dal 2 agosto 2026;**
- **gli obblighi per i sistemi ad alto rischio dell'Allegato III si applicano dal 2 dicembre 2027; quelli per i sistemi dell'Allegato I dal 2 agosto 2028.**

L'articolo 111 regola i sistemi già immessi sul mercato prima di quelle date: restano fuori dal regime finché la loro progettazione non subisce modifiche significative, ma quelli destinati a essere usati da autorità pubbliche devono comunque essere resi conformi entro il **2 agosto 2030**.
Classificare oggi un sistema come ad alto rischio non comporta che sia già inadempiente.
Consente invece di individuare con anticipo gli adempimenti necessari e il momento in cui dovranno essere completati.

Conclusioni

Torniamo alla riunione per la realizzazione di un prodotto.
Alla domanda *“siamo a basso rischio?”* la risposta corretta è un’altra domanda: *“abbiamo seguito il percorso?”*.
Ambito di applicazione, definizione di sistema di AI, finalità prevista, articolo 5, articolo 6 con i suoi allegati, eventuale deroga con il limite della profilazione, articolo 50, eventuale rilievo dei modelli per finalità generali, date di applicazione.
La formula operativa è: ambito, fatto, finalità, norma, allegato, eventuale eccezione, qualificazione, tempo.
Nel prossimo articolo ci fermeremo sul punto che governa gran parte di questo percorso: la finalità prevista.
Vedremo perché, nell’**AI Act**, ciò che il sistema è destinato a fare conta più della tecnologia che contiene, e perché le capacità del sistema, nondimeno, non escono mai davvero di scena.

Articolo del 13 ottobre 2026



La finalità prevista decide più dell'algoritmo

LA FINALITÀ PREVISTA DECIDE PIÙ DELL'ALGORITMO (MA NON LO CANCELLA)

Nell'AI Act la tecnologia, da sola, non determina la qualificazione di un sistema.
È la "finalità prevista" a collegare il sistema al suo uso, al contesto e alle condizioni definite dal fornitore ed è questo collegamento a spiegare perché tecnologie identiche possono ricadere in regimi giuridici molto diversi.
Le capacità del sistema non escono però di scena: contano per i divieti, per la trasparenza, per i modelli per finalità generali e, secondo le linee guida in bozza della Commissione, rientrano nella stessa finalità prevista quando il fornitore presenta il sistema come applicabile a tutto.
Una finalità prevista descritta male non è quindi un problema documentale: può compromettere la classificazione, l'individuazione degli obblighi del fornitore e perfino la posizione del deployer, quando usa il sistema in modo diverso da quanto previsto.

Lo stesso motore, due destini

Prendiamo un modello linguistico e mettiamolo dentro due prodotti diversi.
Nel primo, il sistema suggerisce correzioni grammaticali e stilistiche mentre una persona scrive.
Nel secondo, legge curriculum e lettere di presentazione, assegna a ogni candidato un indicatore di compatibilità con la posizione e propone al selezionatore un ordine di priorità.
Il motore è lo stesso ma il destino giuridico no.
Il correttore non rientra in alcuna area dell'Allegato III, perché la sua finalità prevista non corrisponde a nessuno dei casi d'uso elencati.
E pur generando testo, svolge una funzione di assistenza per l'editing standard, che l'articolo 50, paragrafo 2, dell'**AI Act** esclude dall'obbligo di marcatura, come confermano le linee guida definitive sulla trasparenza del **20 luglio 2026**.
Il sistema per la selezione, invece, ricade nell'Allegato III, punto 4, lettera a): sistemi destinati all'assunzione o alla selezione di persone fisiche, in particolare per analizzare e filtrare le candidature e valutare i candidati; e poiché, nella configurazione descritta, valuta aspetti personali dei candidati per prevederne l'idoneità, effettua profilazione ai sensi dell'articolo 4, punto 4, GDPR: nemmeno la deroga dell'articolo 6, paragrafo 3 dell'AI Act è disponibile in questo caso.
Questo esempio spiega perché parlare di *"rischio dell'algoritmo"* serve a poco.
Il Regolamento disciplina sistemi immessi sul mercato o messi in servizio per svolgere determinate funzioni; non disciplina l'algoritmo in isolamento.

Perché la tecnologia non basta

Quando si parla di intelligenza artificiale l'istinto è guardare alla tecnologia: il modello, le capacità, l'accuratezza, il grado di autonomia, il volume di dati, la capacità generativa.
Sono certamente elementi importanti che, però, non bastano a classificare un sistema ai sensi dell'AI Act.
Il Regolamento guarda continuamente a ciò per cui il sistema è destinato a essere usato; è la *"finalità prevista"*, definita dall'articolo 3, punto 12.
Questo concetto evita un errore frequente che consiste nel classificare un sistema in base alla sua sofisticazione tecnica.
In verità, un sistema molto potente può non essere ad alto rischio mentre un sistema tecnologicamente modesto può esserlo, se è destinato a una funzione compresa nell'Allegato III.

Che cosa deve dire una finalità prevista seria

La finalità prevista non è uno slogan commerciale.
Deve consentire a un terzo di capire quale funzione il sistema svolge e, secondo la definizione, emerge da quattro luoghi che il Regolamento mette sullo stesso piano:
- **le istruzioni per l'uso;**
- **il materiale promozionale o di vendita;**
- **le dichiarazioni del fornitore;**
- **la documentazione tecnica.**

Una descrizione efficace chiarisce almeno:
- **quale attività svolge il sistema e quale output produce;**
- **in quale processo viene utilizzato e da chi;**
- **quali persone possono essere interessate dagli output;**
- **quali decisioni il sistema supporta o influenza;**
- **quali sono le condizioni essenziali di utilizzo.**

"Assistente intelligente per le risorse umane" non dice quasi nulla mentre *"Sistema destinato a classificare le candidature ricevute per una posizione lavorativa e a proporre al recruiter un ordinamento dei candidati sulla base dei requisiti professionali indicati"* dice l'essenziale: chi legge capisce subito di trovarsi nell'Allegato III.

La qualità della finalità prevista è la qualità della classificazione

Le capacità rientrano dalla finestra
Sarebbe però un errore concludere che la tecnologia non conti.
In almeno quattro punti il Regolamento guarda a ciò che il sistema è capace di fare, non solo a ciò per cui è destinato.
I due nuovi divieti dell'articolo 5 introdotti dal *Regolamento (UE) 2026/1744* colpiscono l'immissione sul mercato di sistemi che generano immagini intime non consensuali o materiale pedopornografico non solo quando questa è la loro finalità prevista, ma anche quando la generazione è ragionevolmente prevedibile senza modifiche tecniche significative e mancano garanzie adeguate: è la capacità del sistema, non la destinazione dichiarata, a far scattare il divieto.
L'articolo 50 si applica a chi genera contenuti sintetici o interagisce con le persone, qualunque sia lo scopo commerciale del prodotto.
Il Capo V classifica i modelli per finalità generali anche in base alla potenza di calcolo usata per addestrarli.
Il quarto punto è il più insidioso.
La bozza delle linee guida della Commissione europea sulla classificazione dei sistemi ad alto rischio, pubblicata il **19 maggio 2026** per la consultazione degli stakeholder, propone infatti un criterio che riconduce le capacità del sistema alla sua finalità prevista.
In pratica, quando un sistema per finalità generali viene presentato come ampiamente applicabile, occorre prestare particolare attenzione a come il fornitore descrive i possibili impieghi.
Se gli usi ad alto rischio non vengono esclusi in modo chiaro, concreto e coerente in tutti i materiali informativi e contrattuali, tali usi possono essere considerati ricompresi nella finalità prevista del sistema.
Ciò vale quando tali impieghi risultano tecnicamente fattibili e ragionevolmente prevedibili alla luce delle funzionalità offerte dal sistema.
Pertanto, una clausola nei termini di servizio che *"esclude gli usi ad alto rischio"* non basta, se il posizionamento complessivo del prodotto dice il contrario.
In altre parole: la finalità prevista decide, ma il fornitore non può usarla per nascondere ciò che il sistema sa fare e che il mercato si aspetta che faccia.

Non si può spezzare il sistema per farlo sembrare innocuo

La stessa bozza di linee guida della Commissione europea del **19 maggio 2026** (*documento n.3, paragrafo 75*) chiude un'altra scappatoia.
Quando più sistemi di AI fanno parte di un sistema di AI più complesso e la loro finalità combinata o i loro risultati congiunti influenzano in modo significativo una decisione relativa a una persona, la configurazione complessiva viene considerata come un unico sistema di AI ai fini della classificazione ad alto rischio.
Per evitare che le regole sulla classificazione dei sistemi ad alto rischio vengano aggirate attraverso particolari scelte progettuali, le architetture suddivise in più componenti vengono valutate nel loro insieme.
L'esempio del modello incorporato in due prodotti va letto anche così: ciò che conta è la funzione del sistema finale, non la neutralità del modulo.

Sei uffici, una sola descrizione

La finalità prevista deve emergere in modo coerente dall'intero ecosistema documentale e commerciale del sistema.
Non ha senso scrivere nella documentazione tecnica che il sistema *"organizza documenti"* e poi promuoverlo sul sito come strumento capace di valutare l'affidabilità dei candidati.
Le dichiarazioni del fornitore contribuiscono, per espressa previsione dell'articolo 3, punto 12, a definire il perimetro reale del sistema.
Per questo motivo, classificazione e governance di prodotto devono parlarsi.
Legale, sviluppo, prodotto, marketing, vendite e compliance non possono descrivere lo stesso sistema in sei modi incompatibili e la classificazione non dovrebbe arrivare a valle, a prodotto finito.
Dovrebbe, invece, accompagnare la progettazione e consolidarsi mano a mano che finalità e funzionalità prendono forma.

Quando il deployer cambia il gioco

La finalità prevista resta centrale anche dopo, quando il sistema passa dal fornitore al deployer.
Per i sistemi ad alto rischio, l'articolo 26, paragrafo 1, impone ai deployer di adottare misure tecniche e organizzative idonee a utilizzarli conformemente alle istruzioni per l'uso.
Per gli altri sistemi un obbligo analogo non esiste nell'AI Act, ma la questione si ripresenta da un'altra porta: se il deployer impiega il sistema per una funzione diversa, non cambia soltanto il proprio profilo di rischio.
Può cambiare ruolo.
L'articolo 25, paragrafo 1, prevede tre casi in cui un distributore, un importatore, un deployer o un altro terzo è considerato fornitore di un sistema ad alto rischio, con tutti gli obblighi dell'articolo 16:

- **quando appone il proprio nome o marchio su un sistema ad alto rischio già immesso sul mercato o messo in servizio;**
- **quando apporta una modifica sostanziale a un sistema ad alto rischio, che resta tale;**
- **quando modifica la finalità prevista di un sistema, compreso un sistema per finalità generali, non classificato come ad alto rischio, in modo tale che lo diventi.**

In questi casi il fornitore iniziale cessa di essere considerato tale per quel sistema, ma deve cooperare strettamente con il nuovo fornitore.
Dopo il *Regolamento (UE) 2026/1744* deve mettergli a disposizione la documentazione tecnica necessaria a valutare la conformità, informarlo dei limiti noti e delle modalità di guasto e consentirgli un accesso tecnico mirato, anche per prove e convalida (*paragrafo 2*); la violazione di questi obblighi è ora sanzionata dall'articolo 99.
L'obbligo non sussiste, però, se il fornitore iniziale ha chiaramente specificato che il suo sistema non deve essere trasformato in un sistema ad alto rischio (*paragrafo 2, ultimo comma*).
Per i sistemi multiuso la bozza delle linee guida della Commissione europea del **19 maggio 2026** (*documento 1, paragrafo 21*) distingue due situazioni.
Se il fornitore presenta il sistema come applicabile a tutto e non esclude in modo chiaro e coerente gli usi ad alto rischio, quegli usi si considerano compresi nella finalità prevista e gli obblighi restano suoi.
Se invece li ha esclusi, il deployer che sceglie comunque di impiegare il sistema per un uso dell'Allegato III ne modifica la finalità prevista e diventa fornitore ai sensi dell'articolo 25, paragrafo 1, lettera c), con gli obblighi dell'articolo 16.
In questo secondo caso il fornitore iniziale, avendo escluso espressamente la trasformazione, non è tenuto a cooperare né a consegnare la documentazione.
L'esclusione degli usi ad alto rischio, dunque, non è una clausola di stile: sposta la responsabilità.
Il rilievo operativo è evidente.

Un'organizzazione che acquista un sistema e lo riutilizza per uno scopo diverso non può presumere che la classificazione originaria continui a valere.
Deve riesaminare il quadro e capire se il nuovo uso cambi la qualificazione del sistema, o il proprio ruolo.

La finalità prevista come presidio di governance

La finalità prevista, quindi, non è la frase introduttiva della documentazione ma è un presidio di governance.
Consente al fornitore di delimitare il sistema e consente al deployer di capire entro quale perimetro può utilizzarlo.
Consente, inoltre, alle funzioni di compliance di verificare la classificazione e alle autorità di confrontare ciò che il fornitore dichiara con ciò che il prodotto fa effettivamente e con il modo in cui viene proposto sul mercato.
Da questa prospettiva, una finalità prevista troppo ampia è pericolosa quanto una artificiosamente stretta.
La prima rende impossibile classificare.
La seconda nasconde usi che il prodotto è chiaramente progettato e venduto per svolgere, e che la bozza delle linee guida della Commissione europea riporta dentro la finalità prevista.
La buona finalità prevista è precisa abbastanza da descrivere l'uso reale e stabile abbastanza da governare il ciclo di vita del sistema.

Conclusioni

La classificazione AI Act non deriva dal nome della tecnologia ma dall'incontro tra ciò che il sistema è, ciò che il fornitore dichiara che deve fare, ciò che il mercato è indotto ad aspettarsi e le fattispecie del Regolamento.
Per questo motivo, la finalità prevista è uno snodo decisivo.
Se è confusa, la classificazione diventa confusa.
Se è artificiosamente stretta, le capacità del sistema la riaprono.
Se cambia, può cambiare il regime giuridico e perfino il soggetto che ne risponde.
Nel prossimo articolo affronteremo l'equivoco successivo: un sistema ad alto rischio non è tale perché qualcuno ha calcolato un rischio alto.
Vedremo perché la classificazione dell'articolo 6 dell'AI Act e la gestione dei rischi dell'articolo 9 devono restare separate, e perché l'alto rischio è un regime intero, non un singolo articolo.

Articolo del 15 ottobre 2026


Probabilità
Gravità
1 2 3 4 5
1 1 2 3 4 5
2 2 4 6 8 10
3 3 6 9 12 15
4 4 8 12 16 20
Rischio alto?
Non è così semplice.
AI Act: "Ad alto rischio" non significa avere calcolato un rischio alto
TIONE DEI RISCHI
(Art. 9)
Identificazione e analisi dei rischi
Valutazione e stima
Misure adeguato e mirate
Monitoraggio continuo
L'INTERO REGIME DI PRODOTTO (Capo III)
Requesti derrmai
Governance del duo
Documentazione e registratove
Trasparenza e registrattore
Sinveglianza urtena
Obinnoneuza e accustanei
+
OBBLIGHI DEL FORNITORE
(Art. 16 e seguenti)

AI ACT: "AD ALTO RISCHIO" NON SIGNIFICA AVERE CALCOLATO UN RISCHIO ALTO

"Ad alto rischio" è una categoria giuridica dell'AI Act, non il risultato di una matrice di rischio.
L'articolo 6 del Regolamento stabilisce quando un sistema è classificato ad alto rischio; l'articolo 9 impone, per i sistemi che lo sono, un processo continuo di gestione dei rischi, che è soltanto uno dei requisiti di un regime molto più ampio.
Confondere i due momenti porta a errori di metodo: si finisce per usare la valutazione del rischio per decidere una classificazione che il Regolamento fa dipendere da criteri normativi, finalità e casi d'uso.
Il punto principale in cui un giudizio di rischio entra nella classificazione dei sistemi dell'Allegato III, l'articolo 6, paragrafo 3, è un'eccezione tipizzata, preclusa in caso di profilazione, documentata, registrata e sindacabile.

L'equivoco della matrice

Chi si occupa di compliance conosce bene il foglio di calcolo con le due colonne: probabilità e gravità. Si moltiplicano, si ottiene un numero, si colora la cella. Sopra una certa soglia, il rischio è *"alto"*.
È uno strumento utile. Ma quando arriva l'**AI Act**, quel foglio produce un equivoco: la tentazione di leggere *"sistema ad alto rischio"* come *"sistema per cui abbiamo calcolato un rischio alto"*.
Nel linguaggio comune l'equazione regge. Nell'AI Act no.
Questo articolo spiega perché, e che cosa succede quando si confondono le due cose.

Due domande che non vanno confuse

L'articolo 3, punto 2, definisce il rischio come la combinazione della probabilità del verificarsi di un danno e della gravità del danno stesso. È la definizione classica, quella del foglio di calcolo.
Ma quando l'articolo 6 parla di sistemi *"ad alto rischio"* non usa quella definizione per misurare qualcosa.
Usa, invece, una categoria regolatoria, costruita con criteri specifici: prodotti, casi d'uso, finalità.
Per questo motivo, vanno tenute distinte due domande.
La prima: il sistema ricade nella categoria dell'articolo 6?
La seconda: quali rischi concreti presenta e come vanno gestiti lungo il suo ciclo di vita?
La prima è classificazione. La seconda è risk management.

Prima l'articolo 6, poi l'articolo 9

Il fornitore che vuole sapere se il suo sistema è ad alto rischio non deve aprire una matrice, assegnare probabilità e impatto a una serie di scenari e leggere il numero finale.
Deve aprire l'articolo 6 dell'AI Act che offre due strade.
La prima, al paragrafo 1, è quella dei prodotti: il sistema è un componente di sicurezza di un prodotto dell'Allegato I, e quel prodotto è soggetto a valutazione di conformità da parte di terzi.
La seconda, al paragrafo 2, è quella dei casi d'uso: il sistema rientra in uno dei casi dell'Allegato III.
Se ricorre una delle due, il sistema entra nel percorso dell'alto rischio.
La deroga del paragrafo 3 vale soltanto per la seconda strada.
Un componente di sicurezza dell'Allegato I non può uscire dalla categoria sostenendo di non presentare un rischio significativo: quella porta, per questa tipologia di prodotti, non esiste.
Solo a questo punto entra in gioco l'articolo 9 dell'AI Act, che impone un sistema di gestione dei rischi: un processo continuo e iterativo, pianificato e portato avanti lungo tutto il ciclo di vita del sistema.
L'ordine logico, quindi, è fisso: prima la qualificazione, poi i requisiti applicabili, poi la gestione del rischio.
Non è un ordine cronologico: nella pratica le attività procedono insieme fin dalla progettazione, e la gestione dei rischi accompagna l'intero ciclo di vita del sistema (*articolo 9, paragrafo 2*).

L'articolo 9 non è un'etichettatrice

Che cosa fa, allora, l'articolo 9 dell'AI Act?
Quattro cose:
- **identifica e analizza i rischi noti e ragionevolmente prevedibili;**
- **stima e valuta quelli che possono emergere quando il sistema è usato secondo la finalità prevista, o in condizioni di uso improprio ragionevolmente prevedibile;**
- **impone misure adeguate e mirate;**
- **tiene conto di ciò che emerge dal monitoraggio successivo all'immissione sul mercato.**

È un lavoro sostanziale ma non serve ad assegnare la categoria dell'alto rischio, né a toglierla.
Un sistema che rientra nell'Allegato III resta ad alto rischio anche se, dopo misure robuste, il rischio residuo di alcuni scenari diventa modesto.
La mitigazione riduce il rischio; non cancella la classificazione.
Vale in particolare per la misura più invocata di tutte: "tanto decide una persona".
La bozza delle linee guida della Commissione europea del **19 maggio 2026** (*documento 3, paragrafo 70*) su questo è esplicita.
Il coinvolgimento umano non può, di per sé, impedire che un sistema sia classificato ad alto rischio.

Non è, quindi, una via d'uscita; può al più aiutare a dimostrare, ai fini dell'articolo 6, paragrafo 3, che il sistema svolge una funzione soltanto limitata o preparatoria.
Peraltro, vale anche il contrario.
Un sistema non diventa ad alto rischio perché un'analisi interna ha trovato uno scenario con un danno potenzialmente grave. Anche in questo caso, la risposta sta nelle regole di classificazione e non nel numero della matrice.

L'eccezione dell'articolo 6, paragrafo 3 e le sue regole

L'articolo 6, paragrafo 3, rende la distinzione più sofisticata ma non la cancella.
La norma prevede che un sistema dell'Allegato III non sia 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"*, e se ricorre almeno una delle seguenti quattro condizioni:
- **compito procedurale limitato;**
- **miglioramento del risultato di un'attività umana precedentemente completata;**
- **rilevamento di schemi decisionali o di deviazioni da schemi decisionali precedenti, senza finalità di sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana;**
- **compito preparatorio per una valutazione pertinente ai casi d'uso dell'Allegato III.**

Un sistema che effettua profilazione di persone fisiche è sempre ad alto rischio, qualunque condizione ricorra.
Come va letto l'inciso sull'influenza materiale? Le linee guida in bozza della Commissione europea del **19 maggio 2026** (*documento 3, paragrafo 86*) lo trattano come condizione autonoma di accesso alla deroga e non come semplice esempio: il fornitore deve poter sostenere sia che il sistema non influenza materialmente il risultato decisionale in modo pregiudizievole per le persone, sia che ricorre una delle quattro condizioni.
È la lettura che adotto in questa esalogia, e nella scheda dell'ultimo articolo, perché è la più prudente: una motivazione che regge su entrambi i piani regge anche sulla lettura meno esigente.
Qui, dunque, una valutazione del rischio entra nella classificazione ma non è una matrice libera; è un'eccezione con presupposti determinati, che le citate linee guida leggono in modo restrittivo: chi ordina, punteggia o etichetta gli input come *"utili"* o *"meno utili"* non svolge un compito procedurale limitato; chi produce una raccomandazione o una valutazione specifica non svolge un compito soltanto preparatorio.
Chi applica l'esclusione deve fare tre cose:
- **documentare la valutazione prima dell'immissione sul mercato o della messa in servizio;**
- **registrare il sistema nella banca dati dell'Unione (articolo 49, paragrafo 2);**
- **tenersi pronto a esibire la documentazione alle autorità.**

Con una consapevolezza in più: l'articolo 80 dell'AI Act attribuisce all'autorità di vigilanza del mercato il potere di riesaminare la classificazione adottata dall'operatore.
Se ritiene che il sistema sia stato classificato in modo non corretto, può imporre l'adeguamento ai requisiti applicabili entro un termine stabilito.
E se la classificazione è stata utilizzata per aggirare gli obblighi previsti dal Capo III, possono essere applicate anche le sanzioni dell'articolo 99.
Per questo motivo, la valutazione non è una libera autodichiarazione di "basso rischio" ma è una qualificazione giuridica che deve rispettare criteri precisi e verificabili ed è soggetta al controllo dell'autorità competente.

Un esempio: il ranking dei candidati

Prendiamo, ad esempio, un sistema destinato ad analizzare le candidature per un posto di lavoro e a proporre al recruiter una classifica dei candidati (il cosiddetto ranking).
Il fornitore non parte da una matrice per decidere se l'impatto sia 3, 4 o 5.
Parte dalla finalità prevista e si pone una domanda precisa: questa finalità corrisponde a uno dei casi d'uso dell'Allegato III?
Il punto 4, lettera a), dell'Allegato III elenca i sistemi destinati all'assunzione o alla selezione di persone fisiche, in particolare per analizzare e filtrare le candidature e per valutare i candidati.
Un sistema che legge i curriculum, li confronta con la posizione e ordina i candidati fa esattamente questo.
La risposta, quindi, è sì: il sistema rientra nell'Allegato III.
Poi si chiede se la deroga del paragrafo 3 sia invocabile.
La risposta è no, per due ragioni indipendenti.
La prima: il sistema valuta aspetti personali dei candidati per prevederne l'idoneità, cioè effettua profilazione, e la profilazione chiude la deroga.
La seconda: anche senza profilazione, un ranking per singolo candidato influenza materialmente il risultato della selezione.
Che *"alla fine decida il recruiter"* non cambia nulla: la revisione umana è un requisito di conformità, non un'esimente dalla classificazione.
Il fornitore verifica anche di non sfiorare l'articolo 5: se il sistema inferisse le emozioni dei candidati durante i colloqui, saremmo davanti a una pratica vietata (*paragrafo 1, lettera f*), non a un sistema ad alto rischio.
Solo a questo punto, il fornitore sviluppa il sistema di gestione dei rischi dell'articolo 9, considerando discriminazione, errori, distorsioni dei dati, uso improprio ragionevolmente prevedibile e gli altri rischi per salute, sicurezza e diritti fondamentali.
In altre parole: l'Allegato III è la porta d'ingresso mentre l'articolo 9 governa ciò che accade una volta entrati.

L’alto rischio è un regime, non un articolo

Sarebbe riduttivo pensare che, superata la porta, il fornitore trovi soltanto l’articolo 9 perché, in realtà, trova un intero regime di prodotto.
Infatti ci sono i requisiti della sezione 2 del Capo III:
- **gestione dei rischi (articolo 9);**
- **dati e governance dei dati (articolo 10);**
- **documentazione tecnica (articolo 11);**
- **conservazione delle registrazioni (articolo 12);**
- **trasparenza e informazioni ai deployer (articolo 13);**
- **sorveglianza umana (articolo 14);**
- **accuratezza, robustezza e cibersicurezza (articolo 15).**

Ci sono, poi, gli obblighi del fornitore elencati dall’articolo 16; tra gli altri:
- **il sistema di gestione della qualità (articolo 17);**
- **la conservazione dei documenti (articolo 18);**
- **la valutazione della conformità (articolo 43);**
- **la dichiarazione UE di conformità (articolo 47);**
- **la marcatura CE (articolo 48);**
- **la registrazione nella banca dati dell’Unione (articolo 49);**
- **il monitoraggio successivo all’immissione sul mercato (articolo 72);**
- **la segnalazione degli incidenti gravi (articolo 73).**

E ci sono, a valle, gli obblighi dei deployer dell’articolo 26, di cui parleremo nel prossimo articolo.
Tutto questo si applica dal **2 dicembre 2027** per i sistemi dell’Allegato III e dal 2 agosto 2028 per quelli dell’Allegato I.
La classificazione fatta oggi serve a sapere che cosa costruire da qui ad allora.

Due documenti, non uno

Una governance matura tiene separati almeno due documenti, o due sezioni logicamente distinte.
La prima è la scheda di classificazione normativa che spiega perché il sistema ricade o non ricade negli articoli 5, 6, 50 e nelle altre discipline applicabili, e da quando.
La seconda, quando richiesta, contiene il processo di gestione dei rischi, con metodi, criteri, scenari, misure, rischio residuo e monitoraggio.
Fondere tutto in una sola tabella fa perdere il senso delle due operazioni.
La classificazione deve essere leggibile anche da chi non conosce i dettagli quantitativi della matrice.
Il risk management deve essere abbastanza profondo da governare davvero il sistema nel tempo.

Conclusioni

“Ad alto rischio” non significa *“abbiamo calcolato un rischio alto”* ma significa che il sistema ricade nella categoria giuridica costruita dall’AI Act secondo le regole dell’articolo 6.
Poi, proprio perché è ad alto rischio, il fornitore affronta l’intero regime del Capo III, di cui la gestione dei rischi dell’articolo 9 è il cuore ma non il perimetro.
La formula operativa è: prima classificare, poi applicare i requisiti, valutare, trattare, certificare e monitorare.
Nel prossimo articolo cambieremo punto di osservazione, dal fornitore al deployer.
Vedremo che cosa accade quando il sistema entra in un’organizzazione che deve rispettare i propri obblighi ai sensi dell’AI Act, tratta dati personali e deve effettuare una DPIA ai sensi del GDPR e, in certi casi, una valutazione d’impatto sui diritti fondamentali.

Articolo del 19 ottobre 2026



AI Act, DPIA, FRIA e tre valutazioni che non devono essere confuse

QUANDO ARRIVA IL DEPLOYER: AI ACT, DPIA, FRIA E TRE VALUTAZIONI CHE NON DEVONO ESSERE CONFUSE

Quando un sistema di AI entra in un'organizzazione, il deployer deve capire come è stato qualificato ai sensi dell'AI Act, usarlo nel perimetro previsto e adempiere agli obblighi che il Regolamento assegna a lui, non al fornitore.
Se il sistema è ad alto rischio ai sensi dell'Allegato III e il deployer è un organismo di diritto pubblico, un ente privato che fornisce servizi pubblici o un soggetto che valuta il merito creditizio o determina rischi e prezzi nelle assicurazioni sulla vita e sanitarie, si apre una seconda valutazione: quella d'impatto sui diritti fondamentali (articolo 27).
Se il sistema tratta dati personali e il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone, se ne apre una terza: la DPIA dell'articolo 35 GDPR o, per le autorità di polizia, dell'articolo 23 del d.lgs. 18 maggio 2018, n. 51, che ha recepito la direttiva (UE) 2016/680.
Le tre valutazioni non coincidono. Per il deployer, peraltro, la prima non è una nuova classificazione, ma la verifica di quella del fornitore.
La classificazione riguarda il sistema e il suo uso previsto; la FRIA riguarda l'impatto dell'uso concreto sui diritti delle persone; la DPIA riguarda uno specifico trattamento.
Confonderle produce DPIA deboli, FRIA mancanti e classificazioni improprie.

Il giorno in cui il sistema entra in azienda

Immaginiamo il seguente scenario.
Il fornitore ha consegnato il sistema di AI. Il contratto è firmato, il sistema è installato e la presentazione commerciale ha una slide che dice *"conforme all'AI Act"*.
Ora la palla passa a chi lo userà: un ufficio del personale, un'amministrazione comunale, una banca, un ospedale.
Nel linguaggio del Regolamento, il deployer.
Ed è qui che possono nascere due errori speculari.
Il primo è fidarsi della slide e non chiedere nulla.
Il secondo è pensare che, se il sistema *"è conforme"*, il deployer non abbia altro da fare.
In mezzo c'è il lavoro vero, che questo articolo prova a descrivere.

Che cosa deve arrivare insieme al sistema

Il deployer non dovrebbe trovarsi davanti a una scatola nera, nemmeno dal punto di vista regolatorio.
Deve sapere quale sistema sta usando, quale sia la sua finalità prevista, quali istruzioni lo accompagnino e come sia stato qualificato ai sensi dell'AI Act.
Per i sistemi ad alto rischio, l'articolo 13 impone che il sistema sia progettato in modo sufficientemente trasparente e accompagnato da istruzioni per l'uso che contengono, tra l'altro:

- **la finalità prevista;**
- **il livello di accuratezza;**
- **le circostanze note di rischio;**
- **le misure di sorveglianza umana;**
- **la durata di vita prevista.**

L'articolo 26, dal canto suo, apre gli obblighi del deployer proprio con l'uso conforme a quelle istruzioni (*paragrafo 1*).
C'è poi la banca dati dell'Unione (**articolo 71**), dove sono registrati i sistemi ad alto rischio dell'Allegato III e anche quelli che il fornitore ha ritenuto non ad alto rischio ai sensi dell'articolo 6, paragrafo 3.
Per i deployer pubblici la consultazione non è un'opzione: se accertano che il sistema ad alto rischio che intendono usare non è stato registrato, non lo usano (*articolo 26, paragrafo 8*).
Il deployer, quindi, non inventa da zero la classificazione del sistema acquistato ma acquisisce gli elementi del fornitore, li comprende e verifica che l'uso che intende farne resti nel perimetro previsto.

Verificare non e'riclassificare

Comprendere non vuol dire fermarsi all'etichetta.
Occorre andare oltre e capire su quale base è stata raggiunta la conclusione, domandandosi: qual è la finalità prevista? Il sistema ricade nell'Allegato III? Il fornitore ha applicato l'articolo 6, paragrafo 3? Ha escluso la profilazione? Ha registrato il sistema nella banca dati? Quali sono le istruzioni e i limiti?
Il deployer non subentra al fornitore nelle responsabilità che gli competono.
Tuttavia, non può nemmeno considerare la classificazione del sistema come un dato meramente formale o irrilevante, perché, se tale classificazione dovesse rivelarsi errata, l'autorità di vigilanza del mercato potrebbe rimetterla in discussione: con i poteri generali di vigilanza o, se il fornitore ha invocato l'articolo 6, paragrafo 3, con la procedura dell'articolo 80.
In quel caso, l'organizzazione rischierebbe di scoprire di aver utilizzato un sistema ad alto rischio senza aver adottato le garanzie e le misure di conformità che riteneva, erroneamente, di non dover applicare.

Il problema si fa serio quando il deployer decide di usare il sistema per una finalità diversa.
In quel momento deve chiedersi se il nuovo uso resti compatibile con la qualificazione originaria e se scattino le conseguenze dell'articolo 25 dell'AI Act, che trasformano il deployer in fornitore.

Gli obblighi che il deployer non può delegare

Il deployer di un sistema ad alto rischio non è un semplice utilizzatore.
L'articolo 26 gli assegna obblighi propri:
- **usare il sistema secondo le istruzioni (paragrafo 1);**
- **affidare la sorveglianza umana a persone con la competenza, la formazione e l'autorità necessarie (paragrafo 2);**
- **garantire, nella misura in cui controlla i dati di input, che siano pertinenti e sufficientemente rappresentativi rispetto alla finalità prevista (paragrafo 4);**
- **monitorare il funzionamento, informare il fornitore e, se del caso, sospendere l'uso e segnalare gli incidenti gravi (paragrafo 5);**
- **conservare i log generati automaticamente per almeno sei mesi (paragrafo 6).**

Tre obblighi meritano una menzione a parte, perché riguardano le persone.
Prima di mettere in servizio o usare un sistema ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati (*paragrafo 7*).
I deployer di sistemi dell'Allegato III che adottano decisioni, o assistono nell'adottarle, riguardo a persone fisiche informano queste ultime di essere soggette all'uso del sistema (*paragrafo 11*).
Ancora, la persona destinataria di una decisione presa dal deployer sulla base dell'output di un sistema dell'Allegato III (esclusi quelli del *punto 2*), che produca effetti giuridici o incida in modo analogo significativamente su di lei, e che ritenga abbia un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali, ha diritto di ottenere spiegazioni chiare e significative sul ruolo del sistema nella decisione (*articolo 86*).
È un diritto residuale: non si applica nella misura in cui è già previsto dal diritto dell'Unione (paragrafo 3), e va quindi coordinato con gli articoli 15, paragrafo 1, lettera h), e 22 GDPR, sul cui contenuto la **Corte di giustizia** si è pronunciata nella sentenza *Dun & Bradstreet Austria* (*C-203/22, 27 febbraio 2025*).

Altri obblighi prescindono dall'alto rischio:

- **l'alfabetizzazione del personale, che dopo il 27 luglio 2026 richiede di adottare misure a sostegno dello sviluppo delle competenze (articolo 4);**
- **gli obblighi di trasparenza dell'articolo 50, paragrafi 3 e 4, sui sistemi di riconoscimento delle emozioni, di categorizzazione biometrica e sui deep fake;**
- **i divieti dell'articolo 5, che si rivolgono anche a chi usa il sistema.**

Per il lettore italiano c'è un tassello in più: la legge *23 settembre 2025, n. 132*, all'articolo 11, impone al datore di lavoro o al committente di informare il lavoratore dell'utilizzo dell'intelligenza artificiale, nei casi e con le modalità dell'*articolo 1 bis del d.lgs. 26 maggio 1997, n. 152*.

È un obbligo che si affianca a quello dell'*articolo 26, paragrafo 7*, e che non aspetta il **2 dicembre 2027**.

La seconda valutazione: la FRIA

Prima di usare un sistema ad alto rischio dell'Allegato III (**esclusi quelli per le infrastrutture critiche del punto 2**), alcuni deployer devono fare qualcosa in più.

I deployer che sono organismi di diritto pubblico o enti privati che forniscono servizi pubblici, e i deployer di sistemi per la valutazione del merito creditizio o per la valutazione dei rischi e la determinazione dei prezzi nelle assicurazioni sulla vita e sanitarie (**Allegato III, punto 5, lettere b) e c)), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso del sistema può produrre (articolo 27)**.

È la c.d. **FRIA** (***Fundamental Rights Impact Assessment:* Valutazione d'Impatto sui Diritti Fondamentali**).

La FRIA non è una DPIA con un altro nome.

Descrive i processi del deployer in cui il sistema sarà usato, il periodo e la frequenza dell'uso, le categorie di persone e di gruppi interessati, i rischi specifici di danno per quelle persone, le misure di sorveglianza umana e le misure da adottare se i rischi si concretizzano.

I risultati vanno notificati all'autorità di vigilanza del mercato, compilando il modello di questionario che l'**Ufficio per l'IA** deve predisporre, anche in forma di strumento automatizzato (*paragrafi 3 e 5*).

Il Regolamento stesso costruisce il ponte con la protezione dei dati.

Dopo il *Regolamento (UE) 2026/1744*, se uno qualsiasi degli obblighi dell'*articolo 27* è già soddisfatto dalla DPIA effettuata a norma dell'*articolo 35 GDPR* o dell'articolo 27 della *direttiva (UE) 2016/680*, il deployer può, nella FRIA, rinviare alle sezioni pertinenti della DPIA o riprenderne le parti rilevanti (*paragrafo 4*).

È un meccanismo di coordinamento, non di assorbimento: la *FRIA* resta un adempimento autonomo dell'**AI Act**, con un proprio oggetto e una propria notifica.

Per un'amministrazione pubblica che adotta un sistema ad alto rischio, quindi, i documenti da tenere distinti sono tre: la scheda di classificazione, la *FRIA*, la *DPIA*.

La terza valutazione: la DPIA

Se il sistema tratta dati personali, l'analisi cambia piano.
Il *GDPR* non richiede di stabilire se il sistema sia *"ad alto rischio"* ai sensi dell'AI Act.
Chiede al titolare del trattamento di valutare, quando ricorrono i presupposti dell'articolo 35, l'impatto del trattamento previsto sulla protezione dei dati personali.
Nella pratica i due piani si avvicinano più di quanto sembri.
L'*articolo 35, paragrafo 3, lettera a) GDPR*, rende obbligatoria la **DPIA** per la valutazione sistematica e globale di aspetti personali basata su un trattamento automatizzato, compresa la profilazione, da cui dipendono decisioni con effetti giuridici o analoghi; e l'elenco del Garante, adottato ai sensi dell'*articolo 35, paragrafo 4*, comprende i trattamenti valutativi o di scoring su larga scala e quelli effettuati con tecnologie innovative, tra le quali indica espressamente i sistemi di intelligenza artificiale. Nella selezione del personale, poi, gli interessati sono candidati e lavoratori, cioè persone in posizione di squilibrio rispetto al titolare.
Quindi, per il sistema di selezione del personale dei nostri esempi, la DPIA è di regola dovuta, a prescindere dall'AI Act.
La **DPIA** guarda al trattamento concreto: finalità, categorie di dati, interessati, fonti, flussi, destinatari, conservazione, misure, necessità, proporzionalità e rischi per i diritti e le libertà; e si confronta con l'*articolo 22 GDPR*.
Dopo la sentenza *SCHUFA* della Corte di giustizia (*C-634/21, 7 dicembre 2023*), un punteggio automatizzato sul quale il decisore si basa in modo determinante può costituire esso stesso una decisione automatizzata.
La Corte si è pronunciata su un punteggio prodotto da un terzo, ma il principio è difficilmente eludibile anche per un ranking interno: a mio avviso il *"ranking proposto al recruiter"* non è al riparo soltanto perché a firmare è una persona, e il titolare dovrà verificare se ricorra una delle eccezioni dell'articolo 22, paragrafo 2, con le garanzie del paragrafo 3.
Le due valutazioni, insomma, non si sovrappongono.
Un sistema può non essere ad alto rischio ai sensi dell'*AI Act* e il trattamento presentare comunque un rischio elevato ai sensi del *GDPR*; e un sistema ad alto rischio non consente di saltare la valutazione *GDPR* né di presumere quali siano i rischi del trattamento concreto.

Un ponte, non una fusione: l'articolo 26, paragrafo 9

L'AI Act riconosce espressamente il collegamento tra i regimi.
L'articolo 26, paragrafo 9, prevede che, *"se del caso"*, i deployer di sistemi ad alto rischio usino le informazioni fornite dal fornitore a norma dell'articolo 13 per adempiere al loro obbligo di effettuare una valutazione d'impatto sulla protezione dei dati, ai sensi dell'*articolo 35 GDPR* o dell'*articolo 27 della direttiva (UE) 2016/680*, recepito in Italia dall'articolo 23 del *decreto legislativo 18 maggio 2018, n.51*.
Il rinvio alla direttiva di polizia non è un dettaglio: per le autorità di contrasto la *DPIA* ha una base giuridica diversa, e l'*AI Act* lo sa.
Il legislatore non dice che la classificazione ad alto rischio sostituisce la *DPIA*. Dice che le informazioni sul sistema devono alimentarla.
Il fornitore conosce architettura, finalità prevista, prestazioni, limiti, rischi noti e condizioni di funzionamento.
Il titolare conosce il trattamento concreto, il contesto organizzativo, i dati, gli interessati e le conseguenze reali dell'impiego.
La *DPIA* nasce dall'incontro tra queste due prospettive, ma conserva la propria autonomia giuridica.

Deployer e titolare non sono sinonimi

Un'altra distinzione è necessaria. *"Deployer"* è un termine dell'AI Act.
"Titolare del trattamento" è un termine del *GDPR*.
Possono coincidere nella stessa organizzazione, ma non sono la stessa cosa.
Se il deployer usa il sistema per proprie finalità e determina finalità e mezzi del trattamento, è titolare e, quando ricorrono i presupposti, deve fare la *DPIA*.
Se invece opera come responsabile del trattamento per conto di un titolare, l'obbligo dell'*articolo 35 GDPR* resta in capo al titolare, e il responsabile deve assisterlo secondo l'*articolo 28 GDPR*.
La mappa non finisce qui.
Il fornitore che eroga il sistema come servizio tratta spesso i dati del deployer come responsabile e i propri dati di addestramento come titolare.
Un deployer che modifica la finalità del sistema può diventare fornitore ai sensi dell'articolo 25 senza smettere di essere titolare; e il nuovo articolo 4 bis, introdotto dal *Regolamento (UE) 2026/1744*, che estende a fornitori e deployer di tutti i sistemi la facoltà, già prevista dall'articolo 10, paragrafo 5, di trattare categorie particolari di dati per individuare e correggere le distorsioni, nei limiti della stretta necessità e con garanzie, è un punto di contatto tra i due regimi che la DPIA deve registrare.
Per questo motivo, le mappe dei ruoli *AI Act* e *GDPR* vanno costruite separatamente, e poi messe in relazione.

Come strutturerei una DPIA che usa un sistema di AI

Una *DPIA* ben costruita dovrebbe aprirsi con una sezione dedicata alla qualificazione del sistema ai sensi dell'*AI Act*, senza farne il cuore della valutazione *GDPR*.
In quella sezione indicherei fornitore, sistema, finalità prevista, qualificazione *AI Act* dichiarata, norma applicata, eventuale riferimento all'Allegato III, eventuale uso dell'articolo 6, paragrafo 3, con gli estremi della registrazione nella banca dati, principali istruzioni e limiti, ruolo dell'organizzazione ai sensi dell'*AI Act* ed eventuale *FRIA* effettuata o dovuta.
Poi aprirei la vera valutazione *GDPR*.
Qui analizzerei i rischi per gli interessati derivanti dal trattamento concreto: discriminazione, inaccuratezza, opacità, decisioni automatizzate e loro contestabilità ai sensi dell'articolo 22, eccesso di dati, riutilizzo incompatibile, perdita di controllo, sicurezza, effetti sui diritti, qualità dei dati, bias e ogni altro scenario pertinente.
La classificazione *AI Act* diventa così un input della *DPIA*, non il suo risultato; e la *FRIA*, dove dovuta, può rinviare alle sezioni pertinenti della *DPIA* senza confondersi con essa.

Conclusioni

L'*AI Act* qualifica il sistema e disciplina gli obblighi legati al ruolo e all'uso.
Ad alcuni deployer richiede una valutazione d'impatto sui diritti fondamentali dell'uso concreto.
Il *GDPR* e la direttiva di polizia valutano il trattamento di dati personali e il rischio per i diritti e le libertà delle persone.
Il sistema può essere lo stesso ma i rischi che osserviamo, e i documenti che li governano, sono diversi.
Nel prossimo e ultimo articolo trasformeremo questi principi in uno strumento operativo: una scheda di classificazione *AI Act* che consenta a fornitori e organizzazioni di documentare il percorso seguito, le fonti usate e le condizioni che impongono un riesame.

Articolo del 21 ottobre 2026



La scheda di classificazione AI Act che ogni organizzazione dovrebbe avere

DALLA TEORIA ALLA GOVERNANCE: LA SCHEDA DI CLASSIFICAZIONE AI ACT CHE OGNI ORGANIZZAZIONE DOVREBBE AVERE

Una classificazione affidabile lascia traccia del ragionamento che l'ha prodotta.
Non basta una casella con scritto "ad alto rischio: sì/no".
Serve una scheda che colleghi ambito di applicazione, sistema, ruolo, finalità prevista, pratiche vietate, articolo 6 con i suoi allegati, eventuale esclusione con il limite della profilazione, registrazione, trasparenza, modelli per finalità generali, date di applicazione, fonti e condizioni di riesame.
Questo ultimo articolo propone una struttura concreta, pensata per trasformare la classificazione da adempimento occasionale a processo verificabile lungo il ciclo di vita del sistema.

Un "no" che non si può difendere

Un'ispezione, un audit interno, una richiesta dell'autorità.
Il momento critico arriva quando qualcuno pone una domanda semplice solo in apparenza: *"Perché avete concluso che questo sistema dell'Allegato III non è ad alto rischio?"*
Nell'organizzazione c'è un file, in un repository, con una tabella. In una cella c'è scritto *"no"*.
Nessuno ricorda chi l'abbia scritto, quale versione del sistema descrivesse, quali documenti fossero stati letti.
Quella cella è il problema.
Se quel *"no"* poggia sulla deroga dell'articolo 6, paragrafo 3, l'**articolo 80 dell'AI Act** consente all'autorità di vigilanza del mercato di riesaminare proprio quella conclusione; negli altri casi valgono i suoi poteri generali di vigilanza.
In entrambe le situazioni, una conclusione senza motivazione non si può difendere.

Dalla risposta alla prova

Una buona classificazione non si limita alla conclusione. Scrivere *"sistema non ad alto rischio"* senza spiegare perché produce un'informazione difficile da verificare, difficile da aggiornare e debole in caso di controllo.
La governance chiede qualcosa di diverso: una traccia sintetica ma completa del ragionamento seguito.
Deve essere possibile capire quali fatti sono stati considerati, quali norme applicate, chi ha partecipato alla valutazione, quali documenti sono stati esaminati e quali condizioni imporrebbero un nuovo esame.
Per questo la scheda di classificazione dovrebbe diventare un documento stabile del sistema di governance dell'AI. Vediamo come costruirla, sezione per sezione.

Prima sezione: chi, che cosa, e se l'AI Act si applica

Si parte dagli elementi di base:
- **nome e versione del sistema;**
- **descrizione sintetica delle funzionalità;**
- **organizzazione che lo sviluppa o lo fa sviluppare;**
- **soggetto che lo immette sul mercato o lo mette in servizio con il proprio nome o marchio; ruolo dell'organizzazione ai sensi dell'AI Act (fornitore, deployer, importatore, distributore, fornitore a valle di un modello per finalità generali);**
- **eventuali altri operatori rilevanti; eventuali circostanze dell'articolo 25 che abbiano trasferito il ruolo di fornitore.**

Poi la domanda che nel secondo articolo di questa esalogia abbiamo chiamato *"zero"*: il Regolamento si applica (articolo 2)? Il sistema rientra in un'esclusione, per esempio quella per la sicurezza nazionale o quella per la ricerca? È un componente di sicurezza di un prodotto della sezione B dell'Allegato I, con il regime speciale dell'articolo 2, paragrafo 2?
Sembra semplice ma evita un errore frequente: discutere della classificazione senza aver chiarito se il Regolamento si applichi, chi sia davvero il fornitore e chi assuma gli obblighi.

Seconda sezione: la finalità prevista, scritta per chi non c'era

La sezione successiva contiene la finalità prevista, in forma abbastanza precisa da essere capita da chi non ha partecipato allo sviluppo.
Quale compito svolge il sistema? Quale output produce? In quale processo entra? Chi lo utilizza? Su quali persone o situazioni possono incidere gli output? Quanto pesa sul processo decisionale? Quali sono le condizioni e i limiti di utilizzo? È presentato come strumento specifico o come piattaforma applicabile a tutto?
Questa descrizione va confrontata con istruzioni, documentazione tecnica, materiali commerciali e configurazioni del prodotto.
Le incoerenze si risolvono prima della classificazione, non dopo.

Terza sezione: il percorso normativo, domanda dopo domanda

Qui la scheda ripercorre il cammino del secondo articolo della nostra esalogia, con una breve motivazione e la fonte per ogni risposta:
- **Zero: l'AI Act si applica al sistema, al soggetto e all'uso (articolo 2)?**
- **Prima: il sistema rientra nella definizione dell'articolo 3, punto 1, letta con le linee guida della Commissione del 6 febbraio 2025?**
- **Seconda: la finalità prevista descritta nella seconda sezione è coerente con istruzioni per l'uso, documentazione tecnica e materiale promozionale (articolo 3, punto 12)?**
- **Terza: l'uso previsto rientra in una pratica vietata dall'articolo 5, comprese le due introdotte dal Regolamento (UE) 2026/1744?**
- **Quarta, percorso dei prodotti: ricorrono le due condizioni dell'articolo 6, paragrafo 1, rispetto ai prodotti dell'Allegato I, tenuto conto dei paragrafi 1 bis, 1 ter e 1 quater e della distinzione tra sezione A e sezione B?**
- **Quarta, percorso dei casi d'uso: il sistema ricade in una delle otto aree dell'Allegato III (articolo 6, paragrafo 2)? Se sì, effettua profilazione di persone fisiche? Se la effettua, la deroga è preclusa; se non la effettua, ricorrono i presupposti dell'articolo 6, paragrafo 3?**
- **Quinta: si applicano gli obblighi di trasparenza dell'articolo 50, e quali gravano sul fornitore e quali sul deployer?**
- **Sesta: l'organizzazione è fornitore di un modello per finalità generali, oppure integra un modello altrui? Nel primo caso, quali obblighi del Capo V si applicano; nel secondo, quali informazioni riceve ai sensi dell'articolo 53, paragrafo 1, lettera b), e il sistema è un sistema per finalità generali ai sensi dell'articolo 3, punto 66?**
- **Settima: da quando si applicano gli obblighi individuati, e il sistema rientra nel regime transitorio dell'articolo 111, compreso il termine del 2 agosto 2030 per i sistemi destinati alle autorità pubbliche?**

Quarta sezione: le eccezioni si motivano di più, non di meno

Le conclusioni che alleggeriscono gli obblighi meritano più attenzione, non meno.
Il caso più evidente è l'articolo 6, paragrafo 3 dell'AI Act.
Se il fornitore ritiene che un sistema dell'Allegato III non sia ad alto rischio, la motivazione non può ridursi a una formula come *"impatto limitato"*.
Occorre anzitutto escludere la profilazione.
Occorre poi spiegare, seguendo la lettura delle linee guida della Commissione europea in bozza del **19 maggio 2026**, perché il sistema non presenti un rischio significativo di danno per salute, sicurezza o diritti fondamentali, anche nel senso di non influenzare materialmente il risultato del processo decisionale, e quale delle quattro condizioni ricorra, con elementi che dimostrino, in particolare, che il sistema non ordina, non attribuisce punteggi e non formula raccomandazioni o valutazioni specifiche, che la bozza delle linee guida considera incompatibili con le condizioni della deroga.
L'articolo 6, paragrafo 4, fa di questa documentazione un passaggio esplicito e vi aggiunge la registrazione nella banca dati dell'Unione ai sensi dell'*articolo 49, paragrafo 2*, i cui estremi vanno riportati nella scheda.
L'*articolo 80* ricorda che la conclusione può essere riesaminata dall'autorità di vigilanza e, se elusiva, sanzionata.
Più una conclusione si allontana dalla regola generale, più la motivazione deve essere solida.

Quinta sezione: firma, data e i motivi per riaprire il file

La scheda si chiude con una qualificazione espressa, con gli obblighi principali che ne derivano e con la data dalla quale si applicano.
Ma contiene anche data, versione del sistema, chi ha partecipato alla valutazione, chi l'ha approvata e quando è previsto il riesame.
Soprattutto, elenca gli eventi che impongono una nuova classificazione:
- **cambio della finalità prevista, introduzione di nuove funzionalità, modifica sostanziale, nuovi contesti d'uso;**
- **cambio di ruolo ai sensi dell'articolo 25 dell'AI Act;**
- **modifiche legislative, come quelle introdotte dal Regolamento (UE) 2026/1744;**
- **aggiornamenti degli Allegati con atti delegati (articolo 7) e delle condizioni della deroga (articolo 6, paragrafi 6 e 7);**
- **adozione definitiva delle linee guida della Commissione previste dall'articolo 6, paragrafo 5, o pubblicazione di nuove linee guida;**
- **risultati del monitoraggio successivo all'immissione sul mercato ed evidenze di uso improprio ragionevolmente prevedibile;**
- **esiti della FRIA o della DPIA che rivelino un uso diverso da quello previsto;**
- **entrata in vigore di norme nazionali di adeguamento, in Italia i decreti legislativi attuativi della legge n. 132/2025.**

La classificazione non deve diventare una fotografia dimenticata in un repository. Deve seguire il sistema.
In un'organizzazione strutturata proporrei due livelli documentali.

Il primo è il registro dei sistemi di AI

Censisce sistemi, ruoli, finalità, stato della classificazione, owner, date di applicazione e scadenze.
Per i deployer pubblici dialoga con la banca dati dell'Unione (*articolo 26, paragrafo 8*).

Il secondo è la scheda di classificazione del singolo sistema

Per i sistemi ad alto rischio si collegano poi gli altri documenti richiesti dal Regolamento:
▪ per il fornitore il sistema di gestione dei rischi, la documentazione tecnica, il sistema di gestione della qualità e la valutazione della conformità;
▪ per il deployer le misure dell'articolo 26 e, dove dovuta, la FRIA dell'articolo 27. Per i sistemi che trattano dati personali, la scheda viene richiamata nella DPIA, senza confondere la qualificazione AI Act con la valutazione del rischio GDPR.
Per le organizzazioni italiane, infine, la scheda tiene conto della legge 23 settembre 2025, n. 132, che ha:
▪ designato l'Agenzia per l'Italia digitale (AGID) come autorità di notifica e l'Agenzia per la cybersicurezza nazionale (ACN) come autorità di vigilanza del mercato, ferme le competenze delle autorità di settore;
▪ introdotto obblighi propri, a cominciare dall'informazione ai lavoratori dell'articolo 11.
Per i sistemi biometrici usati a fini di contrasto, gestione delle frontiere, giustizia e processi democratici e per quelli dei *punti 6, 7 e 8 dell'Allegato III, l'articolo 74, paragrafo 8*, dell'AI Act rimette agli Stati membri la scelta tra le autorità di protezione dei dati e altre autorità indipendenti; Va considerato anche il decreto legislativo **9 settembre 2026, n. 160**, in vigore dal **30 settembre 2026**, sull'uso dei sistemi di IA nelle attività di polizia e sulla responsabilità civile e penale.
La documentazione deve quindi essere leggibile da queste autorità nazionali, che sono le prime a poterla chiedere.
Questa architettura evita duplicazioni e, soprattutto, permette di capire quale documento risponde a quale domanda.

Conclusioni

La classificazione *AI Act* dovrebbe concludersi con una decisione motivata, documentata, registrata dove la legge lo richiede, e riesaminabile.
È il passaggio che trasforma una lettura teorica del Regolamento in governance reale.
Il fornitore qualifica il sistema applicando la legge alla finalità prevista e alle caratteristiche concrete.
Il *deployer* verifica il perimetro in cui lo usa e adempie ai propri obblighi.
Il *risk management* governa i rischi concreti.
La *FRIA*, per chi vi è tenuto, valuta l'impatto dell'uso sui diritti fondamentali.
La *DPIA*, quando necessaria, valuta il trattamento di dati personali e i rischi per i diritti e le libertà.
L'esalogia si chiude dove dovrebbe cominciare ogni progetto operativo: non con una piramide colorata, ma con una domanda documentata.
"Quale norma si applica a questo sistema, per questa finalità, in questo contesto, e da quando?"

Articolo del 23 ottobre 2026

Cyber & Cyber

Sicurezza • Dati • Geopolitica

Cyber & Cyber tratta le principali tematiche che alimentano il settore: sicurezza, tecnologie, dati, policy, malware, hacking, difesa nazionale, guerra ibrida e geopolitica. Non insegue la notizia del giorno, ma guarda con particolare attenzione alla ricostruzione di scenari, alla valutazione dei contesti nazionali, all'analisi dei casi di studio, alla descrizione delle tecnologie, agli equilibri internazionali, il tutto nei principali domini fisici: terra, acqua, aria e spazio.
È anche e soprattutto un circuito autorevole di competenze (e un tessuto connettivo di aziende, università, centri di ricerca e singoli professionisti), che promuove occasioni di incontro e confronto come conferenze, workshop e appuntamenti conviviali, tra i membri della community.

CONTATTI

https://cyberandcyber.com

Cyber & Cyber

Cyber &Cyber

cyberandcyber