



Ministero dell'istruzione e del merito

LINEE GUIDA PER L'INTRODUZIONE DELL'INTELLIGENZA ARTIFICIALE NELLE ISTITUZIONI SCOLASTICHE
APPROFONDIMENTO NORMATIVO



Ministero dell'istruzione e del merito

Riferimenti normativi

Al fine di orientare le Istituzioni scolastiche e tutti gli attori coinvolti nell'utilizzo dei sistemi di intelligenza artificiale (di seguito, anche «IA») nel mondo scolastico, si riportano, a seguire, le principali fonti di riferimento, adottate sia a livello europeo che nazionale.

I. FONTI EUROPEE

A livello europeo, il quadro giuridico di riferimento è composto dalle seguenti fonti principali¹:

A) REGOLAMENTO (UE) DEL PARLAMENTO EUROPEO E DEL CONSIGLIO 13 GIUGNO 2024/1689, «CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE E MODIFICA I REGOLAMENTI (CE) N. 300/2008, (UE) N. 167/2013, (UE) N. 168/2013, (UE) 2018/858, (UE) 2018/1139 E (UE) 2019/2144 E LE DIRETTIVE 2014/90/UE, (UE) 2016/797 E (UE) 2020/1828» (di seguito, anche «AI Act» o «Regolamento»), pubblicato sulla Gazzetta Ufficiale dell'Unione europea (GUUE, 2024/1689, 12 luglio 2024)

Il **Regolamento** rappresenta il **primo atto normativo** che istituisce un **quadro giuridico uniforme** per quanto riguarda lo sviluppo, la messa in servizio e l'uso di sistemi di intelligenza artificiale, nell'ottica di assicurare un **livello uniforme di tutela dei diritti e delle libertà** degli interessati e, al contempo, la **diffusione di sistemi di IA antropocentrici e affidabili** che fungano da strumenti per gli individui, con il fine ultimo di migliorare il benessere degli stessi.

L'AI Act, entrato in vigore il 1° agosto 2024, prevede un **regime di applicazione delle disposizioni differenziato, suddiviso tra il 2025 e il 2027**².

¹ Il quadro giuridico europeo in materia di IA si compone di molteplici fonti normative e regolatorie. Di seguito, si riportano le fonti che, per brevità di trattazione, non sono state esaminate nel paragrafo in oggetto: **«Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models»** (Parere 28/2024 su alcuni aspetti della protezione dei dati relativi al trattamento dei dati personali nel contesto dei modelli di IA), dell'*European Data Protection Board* del 17 dicembre 2024; **Direttiva del Parlamento europeo e del Consiglio «sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio»**, del 23 ottobre 2024; **Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law»** adottato dal Consiglio d'Europa e altri firmatari (i.e., Georgia, Islanda, Norvegia, Regno Unito, Israele, Stati Uniti d'America) il 5 settembre 2024; **Decisione C(2023)3215 - Standardisation request M/5932**, adottata dalla Commissione europea il 25 maggio 2023; **Dichiarazione europea sui diritti e i principi digitali per il decennio digitale** (2023/C 23/01), del 23 gennaio 2023; **Risoluzione del Parlamento europeo - «L'intelligenza artificiale in un'era digitale»** del 3 maggio 2022.

² Con riferimento all'entrata in vigore e all'effettiva applicazione dell'AI Act, ai sensi dell'art. 113 del Regolamento medesimo si rappresenta quanto segue: (i) l'AI Act entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea (1° agosto 2024) e si applica a decorrere dal 2 agosto 2026; (ii) i Capi I e II, relativi alle «Disposizioni generali» e alle «Pratiche di IA vietate», si applicano a decorrere dal 2 febbraio 2025; (iii) il Capo III, sezione 4 («Autorità di notifica e organismi notificati»), il Capo V («Modelli di IA per finalità generali»), il Capo VII («Governance»), il Capo XII («Sanzioni») e l'art. 78 («Riservatezza») si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'articolo 101 («Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali»); (iv) l'art. 6, par. 1 («Regole di classificazione per i sistemi di IA ad alto rischio») e i corrispondenti obblighi di cui all'AI Act si applicano a decorrere dal 2 agosto 2027; (v) i sistemi di IA ad alto rischio di cui all'Allegato III, «Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2» e i corrispondenti obblighi di cui all'AI Act si applicano a decorrere dal 2 agosto 2026.

Quanto, invece, al **regime transitorio** da seguire, si rappresenta quanto segue:

- (i) il Regolamento incoraggia i fornitori di sistemi di AI a iniziare a rispettare, su base volontaria, gli obblighi previsti dall'AI Act già durante il periodo transitorio (Considerando 178, AI Act);
- (ii) ai sensi del Considerando 179, AI Act, inoltre:



Ministero dell'istruzione e del merito

Secondo il Considerando 4 del Regolamento, per **intelligenza artificiale** deve intendersi la «**famiglia di tecnologie in rapida evoluzione che contribuisce al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali**. L'uso dell'IA, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali disponibili per i singoli e le organizzazioni, **può** fornire vantaggi competitivi fondamentali alle imprese e **condurre a risultati vantaggiosi sul piano sociale e ambientale**, ad esempio in materia di assistenza sanitaria, agricoltura, sicurezza alimentare, **istruzione e formazione**, media, sport, cultura, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, monitoraggio ambientale, conservazione e ripristino della biodiversità e degli ecosistemi, mitigazione dei cambiamenti climatici e adattamento ad essi».

Con particolare riferimento al mondo istruzione, il considerando 56 del predetto Regolamento (UE) 2024/1689 chiarisce che «**La diffusione dei sistemi di IA nell'istruzione è importante per promuovere un'istruzione e una formazione digitali di alta qualità e per consentire a tutti i discenti e gli insegnanti di acquisire e condividere le competenze e le abilità digitali necessarie**, compresa l'alfabetizzazione mediatica, e il pensiero critico, per partecipare attivamente all'economia, alla società e ai processi democratici».

Al fine di delimitare il **perimetro soggettivo di operatività dell'AI Act**, occorre precisare che il Regolamento medesimo definisce i **ruoli e gli obblighi specifici di tutti gli operatori coinvolti** nello sviluppo di sistemi di IA (ad es., fornitore, distributore, importatore, *deployer*, ecc.) (Considerando 83, AI Act).

In particolare, è possibile distinguere i seguenti ruoli principali:

- **“fornitore”**, definito come «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che **sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio**, a titolo oneroso o gratuito» (art. 3, par. 1, n. 3, AI Act);
- **“deployer”**, definito come «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo **che utilizza un sistema di IA sotto la propria autorità**, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale» (art. 3, par. 1, n. 4, AI Act).

Per altro verso, con riferimento all'**ambito oggettivo** dell'AI Act, è possibile **distinguere** tra **“sistemi di IA”** e **“modelli di IA”**. In particolare:

-
- «il presente regolamento si dovrebbe applicare a decorrere dal 2 agosto 2026. Tuttavia, tenuto conto del rischio inaccettabile associato all'uso dell'IA in determinati modi, i divieti nonché le disposizioni generali del presente regolamento dovrebbero applicarsi già a decorrere dal 2 febbraio 2025 [...]»;
 - le disposizioni sugli organismi notificati e sulla struttura di governance dovrebbero applicarsi a decorrere dal 2 agosto 2025, ritenendosi opportuno che l'infrastruttura relativa alla governance e al sistema di valutazione della conformità sia operativa prima del 2 agosto 2026;
 - gli obblighi per i fornitori di modelli di AI per finalità generali dovrebbero applicarsi a decorrere dal 2 agosto 2025;
 - le disposizioni relative alle sanzioni dovrebbero applicarsi a decorrere dal 2 agosto 2025.
- (iii) i fornitori e i *deployers* dei sistemi di IA ad alto rischio destinati ad essere utilizzati da autorità pubbliche adottano misure necessarie per conformarsi ai requisiti previsti dal Regolamento entro il 2 agosto 2030.



Ministero dell'istruzione e del merito

- a) i **“sistemi di IA”** sono sistemi automatizzati progettati per funzionare con livelli di autonomia variabili, che possono «presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti», deducono dall'input che ricevono «come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali» (art. 3, par. 1, n. 1, AI Act);
- b) i **“modelli di IA”** sono componenti essenziali dei sistemi, i quali, per divenire sistemi di AI, necessitano dell'aggiunta di specifiche componenti, tra cui un'interfaccia utente (Considerando 97, AI Act).

Rispetto ai sistemi/modelli, il Regolamento **vieta espressamente alcune pratiche di IA**, individuate dall'art. 5, par. 1, AI Act, tra cui, a titolo esemplificativo e non esaustivo:

- uso di tecniche subliminali o volutamente manipolative o ingannevoli;
- valutazione o classificazione delle persone fisiche sulla base del loro comportamento sociale o di caratteristiche personali, con attribuzione di un punteggio sociale e conseguente applicazione di trattamenti pregiudizievoli ovvero sfavorevoli.

In particolare, come già anticipato nel paragrafo 1.1. delle Linee Guida, con riferimento al **settore dell'istruzione**, la predetta disposizione **vieta i sistemi di IA che individuino le emozioni di una persona fisica nell'ambito degli istituti di istruzione**, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza (art. 5, lettera f; cfr. Considerando 44).

Ciò posto, il Regolamento adotta un **approccio basato sul rischio**, classificando i **sistemi di IA** in base al rischio che potrebbe essere generato dal loro utilizzo. In particolare, il Regolamento propone **quattro livelli** di classificazione del rischio, così distinti:

- **Rischio inaccettabile**: sono **vietati** tutti i sistemi che violano i valori fondamentali dell'UE e/o i diritti umani e rappresentano una chiara minaccia per la sicurezza e i valori democratici (ad. es., attribuzione di punteggi sociali - c.d. *“social scoring”*; riconoscimento delle emozioni nei luoghi di lavoro e nelle istituzioni educative; identificazione biometrica remota in tempo reale a fini di applicazione della legge in spazi pubblicamente accessibili) (art. 5, par. 1, AI Act);
- **Alto rischio**: si tratta di sistemi di IA che possono comportare **rischi significativi** per la salute, la sicurezza o i diritti fondamentali delle persone. Tali sistemi non sono vietati, ma per la relativa immissione sul mercato sono richiesti **standard elevati di sicurezza, trasparenza e affidabilità**. A titolo esemplificativo e non esaustivo, sono classificati “ad alto rischio” i sistemi di IA utilizzati nei seguenti settori: (i) infrastrutture e nei trasporti; (ii) istruzione e formazione³; (iii) sanitario, con particolare riferimento ai prodotti medicali e alla pratica chirurgica; (iv) accesso all'impiego e al mondo del lavoro; (v) giustizia e pubblica sicurezza (Capo III, AI Act);
- **Rischio limitato**: tale livello si riferisce ai sistemi di IA che presentano un **rischio minore**, ma che devono soddisfare in ogni caso **specifici requisiti** in materia di **trasparenza**, in quanto destinati ad essere utilizzati da persone fisiche. A titolo esemplificativo e non esaustivo, quando si utilizzano

³ Per un maggior approfondimento sui sistemi di IA “ad alto rischio”, anche con specifico riferimento al settore dell'istruzione e della formazione, nonché sui relativi obblighi ascrivibili in capo ai fornitori e ai *deployer* che operano con i sistemi di IA ad alto rischio, si rinvia al paragrafo 1.1 delle Linee guida per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche.



Ministero dell'istruzione e del merito

sistemi di IA come *chatbot*, *deepfake* e assistenti virtuali è fondamentale che essi siano chiaramente e visibilmente etichettati come tali, affinché le persone fisiche interessate siano consapevoli del fatto di stare interagendo con un sistema di IA (art. 50, AI Act);

- **Rischio minimo:** si tratta di sistemi che comportano un **impatto minimo sui diritti o la sicurezza delle persone** (ad es., filtri *antispam*; sistemi di traduzione automatica; correttori ortografici; suggeritore automatico) (art. 95, AI Act).

Con specifico riferimento ai modelli di IA, invece, è possibile distinguere tra:

a) modelli di IA per finalità generali (Capo V, Sez. I-II, AI Act):

Si definisce modello di IA per finalità generali «**un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato da una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle [...]**» (art. 3, par. 1, n. 63, AI Act).

Tra gli obblighi per i fornitori di modelli di IA per finalità generali previsti dagli artt. 53 e 54, nell'AI Act, si richiama, a titolo esemplificativo, l'obbligo di redigere apposita **documentazione tecnica, contenente le informazioni di cui all'Allegato XI** (i.e., i compiti che il modello di IA è destinato a eseguire e il tipo e la natura dei sistemi di IA in cui può essere integrato).

I fornitori di modelli di IA per finalità generali **sono sottoposti alla vigilanza della Commissione europea, dell'Ufficio per l'IA e del Gruppo di esperti scientifici per l'IA**, nel rispetto della disciplina di cui agli artt. 88-94, AI Act;

b) modelli di IA per finalità generali che presentano un rischio sistemico (Capo V, Sez. I-III, AI Act):

Un modello di IA per finalità generali è classificato a rischio sistemico se: (i) presenta **capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati**, compresi indicatori e parametri di riferimento; o (ii) è **qualificato come tale mediante una decisione della Commissione, ex officio** o a seguito di una segnalazione qualificata del gruppo di esperti scientifici (art. 51, par. 1, AI Act).

Oltre agli obblighi generali previsti per i fornitori di modelli di IA per finalità generali, **ai fornitori di modelli che presentano un rischio sistemico si applicano anche ulteriori obblighi** tra cui, a titolo esemplificativo, l'obbligo di **effettuare una valutazione dei modelli in conformità di protocolli e strumenti standardizzati che rispecchino lo stato dell'arte**, anche svolgendo e documentando il test contraddittorio (c.d. *adversarial testing*) del modello al fine di individuare e attenuare i rischi sistemici (art. 55, AI Act)⁴.

⁴ In conformità con la procedura di cui all'art. 52, il fornitore è tenuto a rispettare l'**obbligo di notifica alla Commissione europea**, se il modello di AI per finalità generali presenta capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati. Se il fornitore ritiene che, nonostante le elevate capacità di impatto del modello di AI, il modello non presenti un rischio sistemico, può presentare, unitamente alla notifica, le relative argomentazioni per dimostrarlo (art. 52, par. 1 e 2, AI Act).



Ministero dell'istruzione e del merito

B) CODICE DI BUONE PRATICHE DELL'IA PER FINALITÀ GENERALI

Il Codice di buone pratiche dell'IA per finalità generali è stato pubblicato il 10 luglio 2025 dalla Commissione europea al fine di supportare i fornitori dei modelli di IA per finalità generali a rispettare gli obblighi giuridici della legge sull'IA in materia di sicurezza, trasparenza e diritto d'autore.

Tale Codice costituisce uno strumento facoltativo che i fornitori di modelli di IA possono sottoscrivere al fine di dimostrare la conformità dei propri modelli alle disposizioni previste dall'AI Act.

Nello specifico, il predetto Codice è composto dai seguenti capitoli:

- a) **Trasparenza**: che descrive le tre misure che i soggetti firmatari del Codice si impegnano ad attuare per rispettare gli obblighi di trasparenza previsti dall'articolo 53, par. 1, lettere (a) e (b), e dagli allegati XI e XII dell'AI Act e, in particolare:
 - redazione e aggiornamento di tutte le informazioni inserite all'interno del modello di documentazione messo a disposizione dalla commissione europea per i suddetti soggetti firmatari;
 - pubblicazione di informazioni rilevanti, in base al quale i soggetti firmatari, al momento dell'immissione sul mercato di un modello di intelligenza artificiale di uso generale, devono rendere pubblicamente disponibili, tramite proprio sito web o, se non disponibile, attraverso altri mezzi appropriati, le informazioni di contatto per consentire all'Ufficio IA e ai fornitori a valle di richiedere l'accesso alle informazioni rilevanti;
 - obbligo di garantire la qualità, l'integrità e la sicurezza delle informazioni che gli stessi soggetti firmatari rilasciano. Con riferimento alla redazione, all'aggiornamento e al controllo della qualità e della sicurezza delle informazioni e dei documenti, i soggetti firmatari sono incoraggiati a seguire protocolli consolidati e standard tecnici riconosciuti;
- b) **Diritto d'autore**: che offre ai fornitori soluzioni pratiche per mettere in atto una politica conforme al diritto d'autore dell'UE;
- c) **Sicurezza e protezione**: che individua e descrive pratiche concrete per la gestione dei rischi derivanti dai modelli di IA per finalità generali più avanzati. I fornitori possono fare affidamento sul predetto capitolo al fine di conformarsi agli obblighi previsti dalla legge sull'IA.

Sulla base di quanto specificato dal medesimo Codice i primi due capitoli (trasparenza e diritto di autore) sono rivolti a tutti i fornitori di modelli di IA per finalità generali, mentre il terzo (sicurezza e protezione) è applicabile unicamente per un numero limitato di fornitori dei modelli più avanzati.

C) AI PRIVACY RISKS & MITIGATIONS LARGE LANGUAGE MODELS (LLMs)

Il 10 aprile 2025 l'*European Data Protection Board* ha pubblicato il documento intitolato «*AI Privacy Risks & Mitigations Large Language Models*», che propone una metodologia completa di gestione del rischio, volta a identificare, valutare e mitigare gli eventuali rischi relativi alla protezione dei dati personali derivanti dall'utilizzo di sistemi di IA basati su «*Large Language Models*».



Ministero dell'istruzione e del merito

Tale documento, oltre a dare una descrizione dettagliata dei sistemi LLM e illustrarne i rischi e le possibili misure di mitigazione, fornisce tre diversi **casi d'uso** sulla corretta applicazione del modello di gestione dei medesimi modelli:

- **primo caso d'uso**: un assistente virtuale (chatbot) per le richieste dei clienti;
- **secondo caso d'uso**: un sistema basato su LLM per il monitoraggio e il supporto del progresso degli studenti;
- **terzo caso d'uso**: un assistente AI per la gestione dei viaggi e degli appuntamenti.

D) CONVENZIONE QUADRO DEL CONSIGLIO D'EUROPA SULL'INTELLIGENZA ARTIFICIALE E I DIRITTI UMANI, LA DEMOCRAZIA E LO STATO DI DIRITTO, DEL 5 SETTEMBRE 2024

La Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo stato di diritto rappresenta un documento che si pone quale obiettivo quello di definire delle regole che mirano a garantire che le attività del ciclo di vita dei sistemi di intelligenza artificiale siano pienamente coerenti con i diritti umani, la democrazia e lo Stato di diritto.

Nello specifico, tale Convenzione include una serie di concetti chiave, che devono essere tenuti in considerazione nell'ambito dell'implementazione dei sistemi di IA, comuni anche all'AI Act, quali:

- previsione di un approccio incentrato sull'essere umano, coerente con i diritti umani, la democrazia e lo stato di diritto;
- analisi dei rischi derivanti dall'utilizzo di sistemi di IA;
- necessità di rispettare i principi fondamentali per un'IA affidabile (i.e., trasparenza, robustezza, sicurezza, governance e protezione dei dati);
- previsione di meccanismi per assicurare la trasparenza per i contenuti generati dall'IA e nelle interazioni con i sistemi di IA;
- previsione di documentazione rafforzata;
- supporto all'innovazione sicura attraverso i "sandbox" normativi;
- previsione di obblighi di gestione del rischio;
- previsione di specifici meccanismi di supervisione per il controllo delle attività legate all'IA.

E) LINEE GUIDA SULLE PRATICHE VIETATE IN MATERIA DI INTELLIGENZA ARTIFICIALE (IA), DEL 4 FEBBRAIO 2025, DELLA COMMISSIONE EUROPEA ADOTTATE IN ATTUAZIONE DEL REGOLAMENTO (UE) 2024/1689 (AI ACT)

La Commissione europea ha pubblicato, il 4 febbraio 2025, le linee guida per l'applicazione delle pratiche di intelligenza artificiale vietate, come stabilito dal Regolamento UE 2024/1689 (AI Act). Questo documento fornisce strumenti interpretativi e pratici per l'attuazione dell'articolo 5 dell'AI Act, che disciplina le tecnologie di IA ritenute a rischio inaccettabile.

Le linee guida hanno lo scopo di salvaguardare la dignità umana, l'autonomia decisionale e il benessere, prevenendo pratiche che potrebbero manipolare o ingannare gli individui. Particolare attenzione viene



Ministero dell'istruzione e del merito

dedicata alla protezione delle categorie vulnerabili, come minori e persone con disabilità, più suscettibili a tali forme di sfruttamento.

Tra le pratiche vietate si segnalano quelle che impiegano tecniche subliminali, manipolative o ingannevoli per influenzare in modo dannoso le scelte di un individuo o di un gruppo. Sono vietati anche i sistemi che sfruttano specifiche vulnerabilità legate a età, disabilità o condizioni socioeconomiche.

F) LINEE GUIDA DELLA COMMISSIONE EUROPEA SULLA DEFINIZIONE DI SISTEMI DI IA NELL'AI ACT, DEL 6 FEBBRAIO 2025

Il documento in esame, approvato dalla Commissione europea con provvedimento del 6 febbraio 2025, (C(2025) 924 final) offre una guida sulla definizione di “**sistema di intelligenza artificiale**”, secondo il Regolamento (UE) 2024/1689 (AI Act).

In particolare, le Linee guida chiariscono i **sette elementi chiave** che caratterizzano un sistema di IA e che lo distinguono da *software* di tipo tradizionali, al fine di facilitare l'applicazione coerente della normativa nell'Unione europea. Nello specifico, per definire un “sistema di IA” ai sensi dell’art. 3, par.1, dell’AI Act, devono sussistere i seguenti elementi: (i) il sistema è sviluppato con macchine ed eseguito su di esse; (ii) il sistema è progettato per operare con vari livelli di indipendenza dal controllo umano, anche parziale (autonomia); (iii) il sistema può auto-apprendere e adattarsi dopo la messa in esercizio (adattabilità); (iv) il sistema è volto al raggiungimento di specifici obiettivi definiti in modo esplicito o implicito; (v) il sistema deduce, sulla base di input, come generare output utilizzando tecniche di intelligenza artificiale (capacità di inferenza); (vi) il sistema produce previsioni, contenuti, raccomandazioni o decisioni (output rilevanti); (vii) il sistema di IA è in grado di influenzare contesti fisici o digitali (impatto sugli ambienti).

G) PRIMI ORIENTAMENTI DEL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI SULL'IA GENERATIVA, DEL 3 GIUGNO 2024

Il documento in esame fornisce **linee guida pratiche** alle istituzioni dell’UE per garantire la **conformità al Regolamento (UE) 2018/1725** nell’uso di sistemi di **IA generativa**, con particolare attenzione alla protezione dei dati personali. In particolare, il documento esamina i rischi, le responsabilità e le misure da adottare per garantire un uso conforme, etico e trasparente di queste tecnologie, coprendo aspetti come minimizzazione dei dati, accuratezza, sicurezza, trasparenza e diritti degli interessati.

H) METODOLOGIA PER LA VALUTAZIONE DEI RISCHI E DEGLI IMPATTI DEI SISTEMI DI INTELLIGENZA ARTIFICIALE DAL PUNTO DI VISTA DEI DIRITTI UMANI, DELLA DEMOCRAZIA E DELLO STATO DI DIRITTO (DI SEGUITO, ANCHE «METODOLOGIA HUDERIA»), ADOTTATA DAL COMITATO SULL'INTELLIGENZA ARTIFICIALE (CAI) DEL CONSIGLIO D'EUROPA IL 28 NOVEMBRE 2024

La **HUDERIA** (*Human Rights, Democracy and Rule of Law Impact Assessment*) costituisce una **metodologia non vincolante**, utilizzabile da attori sia pubblici che privati, **per condurre valutazioni sui rischi e sull'impatto dei sistemi di IA**, con particolare attenzione alla tutela dei diritti umani, della democrazia e dello Stato di diritto.

La metodologia HUDERIA adotta un **approccio socio-tecnico**, che considera tutte le fasi del ciclo di vita dei sistemi di IA come influenzate dalla relazione interconnessa tra tecnologia, scelte umane e strutture sociali. Secondo tale approccio, la gestione dei rischi e degli impatti dei sistemi di IA tiene conto sia degli aspetti tecnici dei sistemi medesimi, sia dei contesti sociali, politici, economici, culturali e tecnologici in cui essi operano.



Ministero dell'istruzione e del merito

Nello specifico, la metodologia HUDERIA prevede quattro elementi:

1. **Analisi del rischio basata sul contesto** (“*Context - Based Risk Analysis - COBRA*”): fornisce un approccio strutturato alla raccolta e alla mappatura delle informazioni necessarie per identificare e comprendere i rischi che il sistema di IA potrebbe comportare per i diritti umani, la democrazia e lo Stato di diritto in considerazione del suo contesto socio-tecnico;
2. **Processo di coinvolgimento degli Stakeholder** (“*Stakeholder Engagement Process – SEP*”): propone un approccio per facilitare e rendere operativo il coinvolgimento, ove appropriato, delle parti interessate rilevanti, al fine di ottenere informazioni sulle persone potenzialmente coinvolte e contestualizzare e verificare i potenziali danni e le relative misure di mitigazione;
3. **Valutazione dei rischi e degli impatti** (“*Risk and Impact Assessment – RIA*”): fornisce possibili elementi per la valutazione dei rischi e degli impatti relativi ai diritti umani, alla democrazia e allo stato di diritto;
4. **Piano di Mitigazione** (“*Mitigation Plan - MP*”): fornisce possibili elementi per definire misure di mitigazione e rimedi.

La metodologia HUDERIA, inoltre, prevede specifiche misure da adottare con riferimento ai c.d. “**soggetti vulnerabili**” (ad es., minorenni). A titolo esemplificativo e non esaustivo, nell’ambito della valutazione dei rischi e degli impatti (RIA), la metodologia in esame invita a considerare non solo i rischi di carattere generale, ma anche quelli specifici, legati alla condizione di vulnerabilità dei soggetti coinvolti. A tal fine, viene richiesto di verificare se siano presenti individui o gruppi con caratteristiche tali da esporli maggiormente agli impatti negativi e di valutare in che modo tali soggetti possano subire conseguenze più gravi rispetto ad altri.

I) DECISIONE DELLA COMMISSIONE CHE ISTITUISCE L’UFFICIO EUROPEO PER L’INTELLIGENZA ARTIFICIALE (C/2024/1459), DEL 24 GENNAIO 2024

Nell’ottica di realizzare, gradualmente, un sistema di governance unico per l’IA nell’Unione europea, con la suddetta Decisione è stato istituito l’**Ufficio europeo per l’intelligenza artificiale**⁵, incaricato della vigilanza dei progressi compiuti nel campo dei modelli di intelligenza artificiale, anche per quanto riguarda i modelli di IA per finalità generali e l’interazione con la comunità scientifica.

All’Ufficio europeo per l’IA è altresì attribuito un ruolo fondamentale nello svolgimento di indagini su eventuali violazioni delle norme sui modelli e i sistemi di IA per finalità generali, anche mediante acquisizione di denunce e segnalazioni.

Con il suddetto atto, la Commissione europea ha affidato agli Enti di normazione europei CEN e CENELEC la redazione di norme tecniche europee a vantaggio dei sistemi di intelligenza artificiale in conformità con i principi dell’AI Act.

J) ETHICAL GUIDELINES ON THE USE OF ARTIFICIAL INTELLIGENCE (AI) AND DATA IN TEACHING AND LEARNING FOR EDUCATORS, ADOTTATE DALLA COMMISSIONE EUROPEA NEL SETTEMBRE 2022 (DI SEGUITO, ANCHE «ETHICAL GUIDELINES»)

⁵ Per ulteriori informazioni di dettaglio sull’organizzazione e le funzioni ricoperte dall’Ufficio europeo per l’IA, si rinvia al seguente [link ai-office](#).



Ministero dell'istruzione e del merito

Le *Ethical Guidelines* individuano i **requisiti fondamentali per un IA affidabile nel settore dell'istruzione**. Secondo la Commissione europea «*L'uso dei sistemi di IA risulta potenzialmente in grado di migliorare l'insegnamento, l'apprendimento e la valutazione, di assicurare risultati dell'apprendimento migliori e di aiutare le scuole a operare in maniera più efficiente*» (p. 11) e, per tale ragione, è sempre più necessario un approccio incrementale allo sviluppo e alla diffusione delle nuove tecnologie.

In particolare, nell'elaborazione delle suddette Linee guida sono stati individuati i **principi fondamentali sottesi all'uso etico dell'IA e al trattamento dei dati personali relativi al mondo dell'istruzione** (i.e., intervento umano, equità, benessere, sicurezza, riservatezza, coesione sociale, non discriminazione), che devono **orientare educatori e dirigenti scolastici nelle decisioni relative all'uso dei sistemi di IA nel mondo scolastico**, nell'ottica di assicurare l'affidabilità dei sistemi medesimi.

K) PIANO D'AZIONE PER L'ISTRUZIONE DIGITALE 2021-2027 «RIPENSARE L'ISTRUZIONE E LA FORMAZIONE PER L'ERA DIGITALE», COMUNICAZIONE DELLA COMMISSIONE EUROPEA AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, DEL 30 SETTEMBRE 2020 (DI SEGUITO, ANCHE «PIANO»)

Secondo quanto affermato al punto 4.1 del suindicato Piano, la promozione di **un'istruzione digitale inclusiva e di elevata qualità** deve rappresentare uno sforzo comune dell'intera società, che coinvolga i governi, gli istituti di istruzione e formazione, il settore privato e pubblico.

Tra le azioni principali illustrate dalla Commissione europea nel suddetto Piano volte a sviluppare un ecosistema altamente efficiente di istruzione digitale vi rientra **l'aggiornamento del quadro europeo** delle competenze digitali, al fine di **includervi l'intelligenza artificiale** e le competenze connesse ai dati, nonché la **promozione della comprensione delle tecnologie emergenti** e delle loro applicazioni nell'istruzione, **l'elaborazione di orientamenti etici sull'intelligenza artificiale (IA)** e sull'utilizzo dei dati nell'insegnamento e nell'apprendimento per gli educatori.

L) LIBRO BIANCO SULL'INTELLIGENZA ARTIFICIALE - «UN APPROCCIO EUROPEO ALL'ECCELLENZA E ALLA FIDUCIA» DELLA COMMISSIONE EUROPEA, DEL 19 FEBBRAIO 2020

In considerazione dell'elevato rischio che talune applicazioni di IA presentano per i cittadini, il suddetto **Libro Bianco individua una serie di prescrizioni** che gli operatori economici devono rispettare sia in fase di progettazione che in fase di realizzazione di sistemi di IA, tra cui:

- previsione di un **set di dati di addestramento di sistemi di IA che rispettino i valori e i diritti fondamentali dell'UE**, in particolare, per quanto riguarda la sicurezza e la privacy degli utenti dei sistemi medesimi;
- **obbligo di tenuta della documentazione relativa alle metodologie, alle procedure e alle tecniche di programmazione** e di addestramento, al fine di consentire alle Autorità competenti di effettuare le prove o ispezioni necessarie;
- attivazione di **strumenti giuridici di tutela** da parte dei soggetti che abbiano subito un pregiudizio derivante dall'utilizzo dei sistemi di IA;
- **obblighi informativi, adeguati al contesto specifico**, in ordine alle capacità e alle limitazioni dei sistemi di IA;



Ministero dell'istruzione e del merito

- minimizzazione del rischio mediante la **programmazione e lo sviluppo di sistemi di IA affidabili**;
- **adeguato coinvolgimento dell'uomo** in relazione alle applicazioni di IA ad alto rischio (ad esempio, previsione della convalida di un sistema di IA da parte di un essere umano prima della sua immissione sul mercato).

M) «ORIENTAMENTI ETICI PER UN'IA AFFIDABILE» ELABORATI DAL GRUPPO DI ESPERTI AD ALTO LIVELLO SULL'INTELLIGENZA ARTIFICIALE, DELL' 8 APRILE 2019

Il suddetto documento, elaborato dal gruppo di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione europea nel giugno 2018, mira ad offrire orientamenti per promuovere e garantire **lo sviluppo e la diffusione di sistemi di IA legalità, etici e affidabili dal punto di vista tecnico e sociale**. In particolare, il documento individua i principi etici a cui devono ispirarsi i sistemi di IA, tra i quali si annoverano i seguenti:

- **legalità**, nell'ottica di assicurare un effettivo rispetto delle leggi e dei regolamenti applicabili in materia;
- **sicurezza**, intesa come resilienza agli attacchi a cui i sistemi di IA sono esposti (ad esempio, attacchi mediante *input ingannevoli*, c.d. "*adversarial attack*");
- **non esclusività della decisione algoritmica**, anche mediante l'implementazione di sistemi di **sorveglianza umana** sulle attività dell'IA;
- **affidabilità delle informazioni**, al fine di evitare inesattezze informative;
- **carattere non discriminatorio** delle decisioni algoritmiche e garanzia di adeguata **accessibilità** dei servizi pubblici;
- **trasparenza** delle metodologie di sviluppo e delle funzionalità dei sistemi di IA;
- **riservatezza e protezione dei dati** durante l'intero ciclo di vita del sistema di IA, comprese le informazioni fornite inizialmente dall'utente e quelle generate nel corso della sua interazione con il sistema;
- **sostenibilità sociale ed ambientale** dei sistemi di IA.

II. FONTI NAZIONALI

A livello nazionale, si segnalano i seguenti documenti⁶:

A) «STRATEGIA ITALIANA PER L'INTELLIGENZA ARTIFICIALE 2024-2026» ADOTTATA DAL DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE E DALL'AGENZIA PER L'ITALIA DIGITALE IL 22 LUGLIO 2024

Al fine di supportare il Governo nello sviluppo di una normativa nazionale in materia di IA, è stato redatto da un Comitato di esperti il documento recante «**Strategia Italiana per l'Intelligenza Artificiale 2024-2026**», (a

⁶ A seguire si riportano le ulteriori fonti che compongono il quadro giuridico nazionale in materia di IA: **Dossier XIX Legislatura, «Disposizioni e deleghe al Governo in materia di intelligenza artificiale»** 11 giugno 2024; **Comunicato alla Presidenza** relativo a «**Disposizioni e delega al Governo in materia di intelligenza artificiale**», del 20 maggio 2024; **Focus «Quando l'intelligenza è artificiale»**, Ufficio Valutazione Impatto Senato della Repubblica, luglio 2024.



Ministero dell'istruzione e del merito

seguire, anche **«Strategia»**), adottata dal Dipartimento per la trasformazione digitale e dall'Agenzia per l'Italia Digitale il 22 luglio 2024.

Attraverso un **approccio multidisciplinare**, la Strategia promuove l'utilizzo di **sistemi di IA** nel tessuto produttivo, imprenditoriale, formativo e sociale, nonché nella Pubblica Amministrazione mediante specifiche **azioni strategiche**, strettamente interconnesse e correlate tra loro, suddivise in quattro macroaree (Ricerca, Pubblica Amministrazione, Imprese, **Formazione**), al fine di creare un ecosistema favorevole per l'intelligenza artificiale e, in particolare, di sviluppare un sistema economico migliore e maggiormente efficiente.

Con particolare riferimento alla "Formazione", intesa come *«un processo di **alfabetizzazione sull'IA** che coinvolga la scuola, i lavoratori e i cittadini tutti, con attenzione alle categorie più deboli [...]»* (pagina 29), la Strategia mira a realizzare specifici **«percorsi educativi sull'IA nelle scuole, per preparare le nuove generazioni a un uso attento e consapevole delle nuove tecnologie»** (pagina 39), nell'ottica di avviare:

- percorsi di studio base e avanzati relativi all'IA;
- attività pratiche volte a conseguire abilità nell'utilizzo degli strumenti di IA, *«evidenziando il corretto utilizzo degli stessi sul piano del rispetto degli aspetti etici e sociali, nonché della privacy e della sicurezza cibernetica»*;
- percorsi formativi *ad-hoc*, anche coinvolgendo università, centri di ricerca, associazioni e aziende che abbiano maturato specifiche competenze in iniziative di formazione, soprattutto su tematiche digitali;
- programmi di "mobilità" finalizzate all'interscambio di competenze digitali (i.e. tirocini, *internship*).

La Strategia individua tra gli obiettivi principali da raggiungere nell'ambito della "Formazione" la **«Realizzazione di percorsi educativi sull'IA»**. Per la suddetta finalità, la Strategia indica azioni specifiche strategiche, tra cui:

- avvicinamento dell'IA alla scuola: le Istituzioni scolastiche (in particolare, scuole primarie e secondarie) sono tenute all'attivazione di percorsi formativi per l'alfabetizzazione in materia di IA, rivolti sia al personale docente che agli studenti;
- corsi erogati dagli Istituti Tecnologici Superiori (ITS) focalizzati sull'IA: gli ITS sono tenuti a prevedere strutture adeguate all'erogazione di corsi sull'IA, prestando particolare attenzione al coinvolgimento delle università e delle aziende del settore ICT specializzate nello sviluppo di soluzioni basate sull'IA.

B) «LEGGE RECANTE «DISPOSIZIONI E DELEGHE AL GOVERNO IN MATERIA DI INTELLIGENZA ARTIFICIALE»» (DI SEGUITO, ANCHE «LEGGE SULL'IA»)

In concomitanza con l'adozione dell'AI Act da parte del Parlamento europeo, il Consiglio dei ministri nella seduta del 23 aprile 2024 ha deliberato un disegno di legge che disciplina l'uso dell'IA nei settori demandati dal Regolamento all'autonomia normativa degli Stati Membri. L'iter di approvazione ha preso avvio con la presentazione del disegno di legge al Senato il 20 maggio 2024 (A.S. 1146) ed è proseguito con l'approvazione in prima lettura il 20 marzo 2025, nonché con la successiva approvazione, con modificazioni, dalla Camera dei deputati in data 25 giugno 2025 (A.C. 2316).



Ministero dell'istruzione e del merito

In particolare, come precisato nella Relazione «*Analisi del quadro normativo in materia di intelligenza artificiale*» del Dipartimento per il programma di Governo della Presidenza del Consiglio dei Ministri, del 31 maggio 2024, **«il D.D.L. sull'IA è la prima proposta legislativa in Europa tesa ad adottare le disposizioni del nuovo AI Act. Introduce criteri regolatori, norme di principio e di settore, che promuovono l'utilizzo delle nuove tecnologie prevedendo, al contempo, misure in grado di contenere il rischio connesso al loro uso improprio o dannoso»**.

Tale **disegno di legge è stato approvato in via definitiva** dal Senato il 17 settembre 2025 (A.S. 1146-B).

La finalità della Legge sull'IA è di porre al centro di ogni attività che riguardi lo sviluppo e l'utilizzo dei sistemi e dei modelli di intelligenza artificiale **il rispetto dell'autonomia e del potere decisionale dell'uomo**, che consente di adottare scelte consapevoli in merito all'utilizzo dei sistemi di IA.

La Legge sull'IA, in particolare, si compone di 28 articoli, volti a **«sostenere e promuovere lo sviluppo di sistemi di intelligenza artificiale che, in armonia con l'apposito regolamento europeo, e gli indirizzi governativi e parlamentari nazionali, siano basati su una visione antropocentrica, nonché su principi di trasparenza, responsabilità, equità e rispetto per i diritti fondamentali, che garantiscono un equilibrio tra le opportunità che offrono le nuove tecnologie e i rischi legati al loro uso improprio, al loro impiego dannoso e anche al loro sottoutilizzo»** (Dossier XIX Legislatura, Camera dei Deputati, 19 giugno 2025).

Ciò posto, le disposizioni della suddetta Legge si innestano, in modo differenziato, a seconda dei singoli settori, nelle diverse fasi del ciclo di vita dell'intelligenza artificiale, dalla ricerca fino all'adozione e al concreto utilizzo dei sistemi e dei modelli di IA.

In particolare, l'articolo 1 enuncia le finalità e l'ambito di applicazione della disciplina prevista dalla Legge sull'IA, sottolineando la **dimensione antropocentrica dell'utilizzo dell'intelligenza artificiale** e della vigilanza sui rischi economici e sociali nonché sull'impatto in ordine ai diritti fondamentali.

L'articolo 3 definisce i principi generali, quali, tra gli altri, il **rispetto dei diritti fondamentali e delle libertà** previsti dall'ordinamento italiano ed europeo e dei principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.

L'art. 24, commi 1 e 2, lett. g), i) e l)⁷, reca principi e criteri direttivi specifici per l'esercizio della delega legislativa al Governo, per l'adozione entro dodici mesi dall'entrata in vigore della Legge di uno o più decreti legislativi che adeguino la normativa nazionale all'AI Act **in materia di istruzione scolastica, formazione superiore e ricerca**, tenendo in considerazione, in particolare, i seguenti aspetti:

⁷ Nello specifico, **in materia di istruzione**, secondo quanto riportato nella Relazione Illustrativa al DDL, «*le lettere g), i) ed l) recano principi e criteri direttivi specifici per l'esercizio della delega legislativa in materia di istruzione scolastica, formazione superiore e ricerca. Tali principi e criteri direttivi fanno riferimento: al potenziamento, all'interno dei curricula scolastici, dello sviluppo di competenze legate alle discipline STEM, nonché artistiche, al fine di promuovere la scelta di percorsi di formazione superiore relativi alle menzionate discipline (lettera g)); alla previsione, nei corsi universitari e delle istituzioni AFAM, nonché nei percorsi di istruzione tecnologica superiore offerti dagli ITS Academy, di attività formative per la comprensione tecnica e l'utilizzo consapevole anche sotto il profilo giuridico delle tecnologie, anche con riferimento ai sistemi di intelligenza artificiale così come definiti dalla disciplina europea, nonché per la corretta interpretazione della produzione di tali sistemi in termini di previsioni, contenuti, raccomandazioni o decisioni (lettera i)); alla valorizzazione delle attività di ricerca e di trasferimento tecnologico in materia di intelligenza artificiale svolte da università, istituzioni dell'AFAM, ITS Academy ed enti pubblici di ricerca, mediante disposizioni finalizzate al perseguimento di alcuni obiettivi specificamente indicati (lettera l))»*.



Ministero dell'istruzione e del merito

- *«potenziamento, all'interno dei curricoli scolastici, dello sviluppo di competenze scientifiche, tecnologiche, ingegneristiche e matematiche legate alle discipline STEM, nonché artistiche, al fine di promuovere la scelta da parte delle studentesse e degli studenti, anche attraverso mirate attività di orientamento personalizzato, di percorsi di formazione superiore relativi alle menzionate discipline» (lettera g);*
- *«previsione, nei corsi universitari e delle istituzioni di alta formazione artistica, musicale e coreutica (AFAM), nonché nei percorsi di istruzione tecnologica superiore offerti dagli istituti tecnologici superiori (ITS Academy), coerentemente con i rispettivi profili culturali e professionali, di attività formative per la comprensione tecnica e l'utilizzo consapevole anche sotto il profilo giuridico delle tecnologie, anche con riferimento ai sistemi di intelligenza artificiale come definiti dalla disciplina europea, nonché per la corretta interpretazione della produzione di tali sistemi in termini di previsioni, contenuti, raccomandazioni o decisioni» (lettera i);*
- *«valorizzazione delle attività di ricerca e di trasferimento tecnologico in materia di intelligenza artificiale svolte da università, istituzioni AFAM, ITS Academy ed enti pubblici di ricerca, mediante disposizioni finalizzate al perseguimento dei seguenti obiettivi: 1) agevolare il coinvolgimento del sistema dell'università e della ricerca nella promozione, nella realizzazione e nell'utilizzo di spazi di sperimentazione normativa in collaborazione con il mondo produttivo; 2) incentivare le attività di supporto esemplificare gli strumenti di collaborazione tra il sistema dell'università e della ricerca e degli ITS Academy e le Autorità nazionali di cui all'articolo 20» (lettera l).*

C) LINEE GUIDA AGID PER L'ADOZIONE DI IA NELLA PA, DEL 17 FEBBRAIO 2025, ATTUALMENTE NON ANCORA ADOTTATE IN VIA DEFINITIVA

Le Linee guida in esame, previste dal D.P.C.M. del 12 gennaio 2024, recante *“Piano triennale per l'informatica nella pubblica amministrazione 2024-2026”*, sono state oggetto di consultazione nei mesi di febbraio e marzo 2025 e attualmente non sono state ancora adottate in via definitiva.

Il documento, che si rivolge, tra gli altri, alle Pubbliche Amministrazioni di cui all'art. 1, comma 2, del D. Lgs. n. 165/2001 e, dunque, anche alle Istituzioni scolastiche, disciplina le **modalità di adozione dei sistemi di Intelligenza Artificiale** con particolare riferimento agli aspetti di conformità normativa e di impatto organizzativo, anche mediante l'individuazione dei principi cui devono attenersi nell'implementazione dei sistemi di IA (i.e., protezione dei dati personali, responsabilità, accessibilità, inclusività, non discriminazione, trasparenza e informazione).

Tali Linee Guida, inoltre, tracciano alcune delle finalità per le quali le Pubbliche Amministrazioni possono adottare l'IA e, in particolare, al fine di:

- automatizzare attività semplici e ripetitive di ricerca e analisi delle informazioni, liberando tempo di lavoro per attività a maggior valore;
- aumentare le capacità predittive, migliorando il processo decisionale basato sui dati;
- supportare la personalizzazione dei servizi incentrata sull'utente, aumentando l'efficacia, l'efficienza e la tempestività dei servizi pubblici anche attraverso meccanismi di proattività;



Ministero dell'istruzione e del merito

- promuovere l'innovazione dei servizi pubblici e dei processi amministrativi.

Le Linee Guida, in conformità con la normativa adottata a livello europeo, suggeriscono altresì l'adozione da parte delle Amministrazioni di strumenti operativi utili al fine di garantire il rispetto della suddetta disciplina come la **FRIA** (*Fundamental Rights Impact Assessment* - Valutazione d'Impatto sui Diritti Fondamentali), i cui risultati devono essere documentati e condivisi con le parti interessate, e i **codici etici**.

Nello specifico, i codici etici e di condotta, possono essere adottati ai sensi dell'art. 95, par. 3 dell'AI Act, dalle Amministrazioni sia in qualità di fornitori sia di *deployer*, favorendo, nel processo di definizione degli stessi, il coinvolgimento dei portatori di interesse, anche privati (organizzazioni rappresentative della società civile, università, centri di ricerca associazioni di fornitori, enti regolatori).

Il contenuto dei codici etici e di condotta può riguardare la previsione di elementi e requisiti supplementari per lo sviluppo e l'utilizzo di sistemi di IA, che si aggiungono a quelli già obbligatori in forza della normativa applicabile. In particolare, ai sensi dell'art. 95, par. 1, dell'AI Act, i codici etici e di condotta dovrebbero incentivare l'applicazione volontaria a tutti i sistemi di IA adottati dalla PA, diversi dai sistemi di IA ad alto rischio, di alcuni o di tutti i requisiti di cui al capo III, sezione 2 dell'AI Act.

D) PIANO TRIENNALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE 2024-2026 ADOTTATO DALL'AGENZIA PER L'ITALIA DIGITALE A DICEMBRE 2023 (DI SEGUITO, ANCHE «PIANO TRIENNALE AGID 2024-2026» O «PIANO TRIENNALE»)

Il Piano Triennale per l'informatica nella Pubblica Amministrazione è uno strumento fondamentale per promuovere la trasformazione digitale del Paese attraverso quella della Pubblica Amministrazione italiana.

Fin dalla sua prima edizione (2017-2019), il Piano triennale ha rappresentato il documento di supporto e di orientamento per le pubbliche amministrazioni italiane (a seguire, anche «**Pubbliche Amministrazioni**» o «**PP.AA.**») nella pianificazione delle attività in materia di innovazione tecnologica e ha costituito il riferimento per declinare le singole strategie che si sono susseguite nel tracciato operativo dallo stesso indicato.

Il nuovo Piano triennale si inserisce in un contesto di riferimento più ampio definito dal programma strategico «*Decennio Digitale 2030*», istituito dalla Decisione (UE) 2022/2481 del Parlamento Europeo e del Consiglio del 14 dicembre 2022, i cui obiettivi sono articolati in quattro dimensioni: competenze digitali, servizi pubblici digitali, digitalizzazione delle imprese e infrastrutture digitali sicure e sostenibili.

In materia di intelligenza artificiale, il suddetto Piano Triennale individua i **principi generali per l'utilizzo dei sistemi di IA nella Pubblica Amministrazione**. In particolare:

- **miglioramento dei servizi e riduzione dei costi:** orientamento degli investimenti in tecnologie di intelligenza artificiale da parte delle PP.AA. nell'ottica dell'automazione dei compiti ripetitivi connessi ai servizi istituzionali obbligatori e al funzionamento dell'apparato amministrativo;
- **analisi del rischio:** valutazione dei rischi associati all'impiego di sistemi di IA al fine di assicurare che tali sistemi non provochino violazioni dei diritti fondamentali della persona o altri danni rilevanti;
- **trasparenza, responsabilità e informazione:** realizzazione di un'attività informativa da parte delle PP.AA. al fine di consentire agli utenti di prendere decisioni consapevoli riguardo all'utilizzo dei servizi che sfruttano l'intelligenza artificiale;



Ministero dell'istruzione e del merito

- **inclusività e accessibilità:** rispetto dei principi di equità, trasparenza e non discriminazione nell'utilizzo di tecnologie di IA, in considerazione delle responsabilità e delle implicazioni etiche ad esse associate;
- **privacy e sicurezza:** adozione da parte delle PP.AA. di standard elevati di sicurezza e protezione dei dati personali, al fine di garantire che i dati dei cittadini siano gestiti in modo sicuro e responsabile;
- **formazione e sviluppo delle competenze:** promozione degli investimenti nella formazione e nello sviluppo delle competenze necessarie ad un utilizzo efficace dell'IA nell'ambito dei servizi pubblici;
- **sostenibilità:** valutazione degli impatti ambientali ed energetici legati all'adozione di tecnologie di intelligenza artificiale e adozione di soluzioni sostenibili dal punto di vista ambientale;
- **dati:** valutazione, da parte delle PP.AA. che acquistano servizi di intelligenza artificiale tramite interfacce per la programmazione delle applicazioni (API), delle modalità e delle condizioni con le quali il fornitore del servizio gestisce i dati forniti dall'amministrazione, con particolare riferimento alla proprietà dei dati e alla conformità con la normativa vigente in materia di protezione dei dati personali.

Ai fini di una corretta regolamentazione dei sistemi di IA e in linea con quanto previsto dall'art. 95 dell'AI Act, il Piano rinvia a specifici codici di condotta, che saranno adottati in materia.

E) PROGRAMMA STRATEGICO INTELLIGENZA ARTIFICIALE 2022-2024, A CURA DEL MINISTERO DELL'UNIVERSITÀ E DELLA RICERCA, DEL MINISTERO DELLO SVILUPPO ECONOMICO E DEL MINISTRO PER L'INNOVAZIONE TECNOLOGICA E LA TRANSIZIONE DIGITALE, DEL 24 NOVEMBRE 2021

Con specifico riferimento al mondo "istruzione e formazione", il suddetto **Programma annovera il "Sistema educativo" tra i "Settori prioritari"** ed evidenzia, al riguardo, la necessità di *«formare i cittadini a questa tecnologia attraverso un nuovo piano di istruzione per comprendere, rafforzare, integrare e diffondere la tecnologia IA. L'intelligenza artificiale dovrebbe essere un argomento importante a tutti i livelli di istruzione. Allo stesso tempo, l'IA può costituire un potente strumento per trasformare il sistema educativo nazionale sviluppando piani di apprendimento personalizzati nei limiti dei principi di equità e affidabilità»*.

Per le suddette finalità, il Programma, tra le principali azioni previste, intende promuovere i talenti e rafforzare le competenze nei seguenti ambiti:

- **corsi e carriere in materie STEM:** integrazione di attività, metodologie e contenuti finalizzati allo sviluppo delle materie STEM nei curricula di tutti i cicli scolastici;
- **sviluppo dell'IA negli Istituti tecnici superiori (ITS):** implementazione dei corsi di programmazione e inclusione di corsi e stage di IA applicata in tutti i curricula ITS.