liquid LAW

VADEMECUM IA A SCUOLA

L'Intelligenza Artificiale (IA) sta rivoluzionando il settore dell'istruzione, offrendo nuove opportunità per personalizzare l'apprendimento in base alle esigenze specifiche del singolo studente, oppure offrendo un valido aiuto per ottimizzare i servizi amministrativi e, in generale, per migliorare l'efficienza didattica. Questo mondo di opportunità, però, è accompagnato da un quadro significativo e rilevante di rischi per i diritti degli utilizzatori.

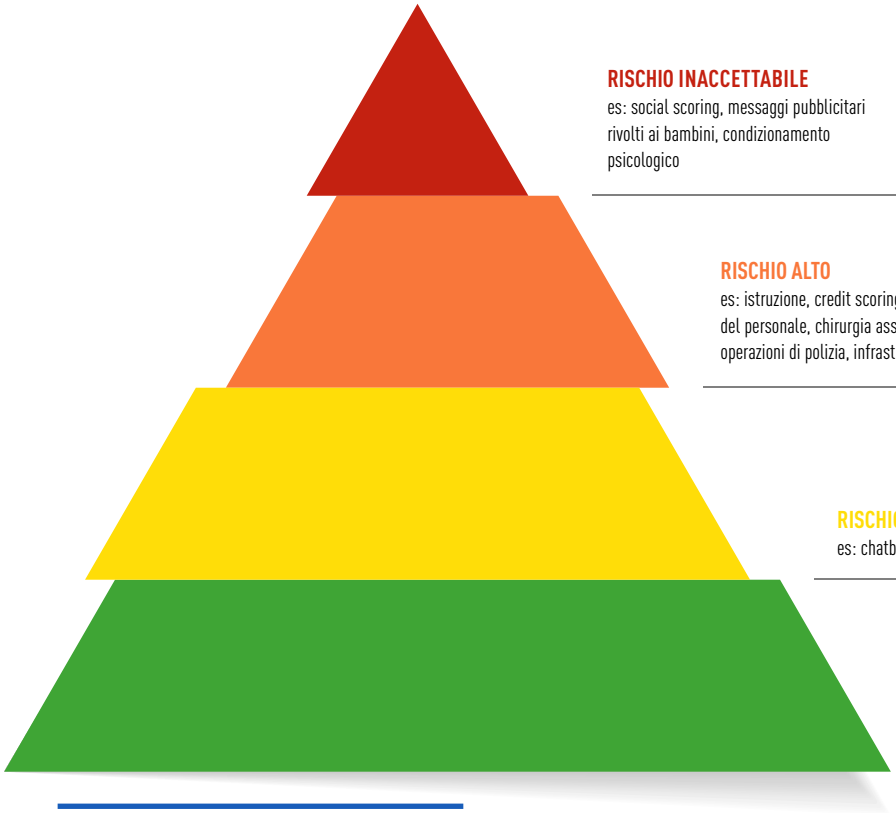
Il presente Vademecum nasce con l'obiettivo di fornire una pratica panoramica per indirizzare l'utilizzo dell'IA nel settore scolastico in modo responsabile e conforme alle normative vigenti.

AI ACT: LIVELLI DI RISCHIO

Con l'entrata in vigore il giorno 1 agosto 2024 dell'**AI ACT** (**Regolamento UE 1689/2024**[1]), l'Unione Europea si è dotata di una sua disciplina in tema IA. Il Regolamento mira, nello specifico, a garantire che i sistemi di IA siano sviluppati e utilizzati in modo sicuro e rispettoso dei diritti fondamentali.

Esso classifica i sistemi di IA in base al livello di rischio associato e garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA.

Nel documento si distinguono quattro categorie di rischio, a seconda del loro potenziale impatto sui diritti dei cittadini:



RISCHIO INACCETTABILE
es: social scoring, messaggi pubblicitari rivolti ai bambini, condizionamento psicologico

VIETATO

RISCHIO ALTO
es: istruzione, credit scoring, selezione del personale, chirurgia assistita, operazioni di polizia, infrastrutture critiche

PERMESSO, nel rispetto di requisiti IA e valutazione di conformità preventiva

RISCHIO LIMITATO
es: chatbot

PERMESSO, nel rispetto di obblighi di trasparenza e informazione

RISCHIO MINIMO O NULLO
es: videogiochi, sistemi antispam

PERMESSO SENZA OBBLIGHI, ma con un codice di condotta suggerito

[1] Testo disponibile su: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Esaminiamoli in modo puntuale:

1. i sistemi di IA classificati come ***rischio inaccettabile***[2] sono vietati perché considerati una minaccia per i diritti fondamentali, la sicurezza e i valori democratici (al loro interno vi rientrano, ad es.: sistemi di punteggio sociale che valutano i cittadini in base al loro comportamento, sistemi di manipolazione subliminale che influenzano le decisioni delle persone senza che ne siano consapevoli; tecnologie di identificazione biometrica in spazi pubblici, con alcune eccezioni per la sicurezza nazionale); in base alla Comunicazione della Commissione - Linee guida della Commissione UE sulle pratiche vietate di intelligenza artificiale stabilite dal Regolamento (UE) 1689/2024[3] esistono dei **casi specifici di IA inaccettabile nel settore dell'istruzione**, come i sistemi in grado di **riconoscere le emozioni**[4];

2. i sistemi ad ***alto rischio***[5], ossia quelli che hanno un impatto significativo sui diritti fondamentali delle persone, possono essere implementati nell'organizzazione solo nel rispetto di obblighi rigorosi in termini di ***trasparenza, sicurezza e supervisione umana***. Tali obblighi[6] ricadono anche **in capo ai meri utilizzatori dei sistemi, come le scuole**: i c.d. ***deeployer***, che dall'AI ACT vengono definiti come "*qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di AI sotto la propria autorità, eccetto quando il sistema di AI è utilizzato nell'ambito di un'attività personale non professionale*"[7]. Particolarmente rilevante per il settore scolastico risulta essere l'**allegato III** del Regolamento che, nell'elencare i sistemi ad alto livello di rischio, alla lettera a), fa riferimento al **settore dell'istruzione e della formazione** all'interno del quale possono rientrare:

a. **sistemi di valutazione automatizzata di compiti, esami o performance degli studenti**: (come software che analizzano esami e compiti per determinare punteggi e voti);

b. **piattaforme di orientamento scolastico e professionale basate su IA** (come sistemi che suggeriscono percorsi di studio o carriere in base a dati degli studenti);

c. **strumenti di apprendimento adattivo che personalizzano i contenuti didattici** (come software che modificano automaticamente i contenuti didattici in base alle prestazioni degli studenti)[8];

---

[2] Art. 5.

[3] Per una loro lettura, si rinvia a: https://digital-strategy.ec.europa.eu/it/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

[4] Si riporta la casistica considerata dalla Commissione nel documento:
- un'applicazione basata sull'IA che utilizza il riconoscimento delle emozioni per l'apprendimento di una lingua online al di fuori di un istituto scolastico non è vietata. Al contrario, se gli studenti sono obbligati da un istituto scolastico a utilizzare l'applicazione, l'uso di tale sistema di riconoscimento delle emozioni è vietato;
- un istituto scolastico che utilizza un software di tracciamento oculare basato sull'intelligenza artificiale durante l'esame online degli studenti per tracciare il punto di fissazione e il movimento degli occhi (punto di sguardo, ad es. per rilevare se viene utilizzato materiale non autorizzato) non è vietato, perché il sistema non identifica o deduce le emozioni. Al contrario, se il sistema viene utilizzato anche per rilevare le emozioni, come l'eccitazione emotiva e l'ansia, questo rientrerebbe nell'ambito del divieto;
- l'utilizzo di un sistema di intelligenza artificiale per il riconoscimento delle emozioni da parte di un istituto scolastico per dedurre l'interesse e l'attenzione degli studenti è vietato. Al contrario, se utilizzato solo a scopo di apprendimento nel contesto di un gioco di ruolo (ad es., per l'addestramento degli attori o per la formazione degli insegnanti), i sistemi di riconoscimento delle emozioni sono consentiti se i risultati non possono influire sulla valutazione o sulla certificazione della persona addestrata;
- l'utilizzo di un sistema di intelligenza artificiale per il riconoscimento delle emozioni da parte di un istituto scolastico durante i test di ammissibilità per i nuovi studenti è vietato;
- l'utilizzo di un sistema di intelligenza artificiale che consente di riprendere gli studenti che parlano tra loro attraverso i loro telefoni o altri canali durante le lezioni online da parte di un istituto di istruzione non è vietato, poiché non deduce le emozioni. Al contrario, se il sistema viene utilizzato anche per rilevare emozioni, come l'eccitazione emotiva, l'ansia e l'interesse, questo rientrerebbe nell'ambito del divieto;
- è vietato a un istituto di istruzione impiegare un sistema di intelligenza artificiale per il riconoscimento delle emozioni sia sugli insegnanti (luogo di lavoro) che sugli studenti (istruzione).

[5] Art. 6 e Allegato III.

[6] I *deployer* sono tenuti, ad es., a: verificare la conformità globale del sistema, assicurandosi che essi siano conformi alle disposizioni dell'AI Act; garantire la supervisione umana implementando meccanismi specifici di monitoraggio e controllo umano; fornire una formazione adeguata a tutti gli operatori dell'organizzazione di riferimento.

[7] Si veda il Considerando 13 dell'AI ACT.

[8] Ad ulteriore chiarimento del contenuto dell'Allegato III, nel Considerando 56 si legge: "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. »

3. i sistemi a ***rischio limitato***[9], ovvero quelli che presentano rischi minimi per i diritti fondamentali, richiedono comunque un certo livello di trasparenza per garantire che gli utenti siano informati sul loro utilizzo (vi rientrano ad esempio *chatbot* e assistenti virtuali);

4. i sistemi a ***rischio minimo***, non sono soggetti a regolamentazioni specifiche o di particolare importanza.

TEMPI DI ATTUAZIONE

L'**AI Act** prevede un'applicazione graduale nel corso del tempo, con una chiara linea temporale entro la quale far divenire effettivi gli obblighi citati nelle varie disposizioni.

In particolare:

- Il **2 febbraio 2025** sono diventati effettivi i **divieti per l'immissione sul mercato dell'AI vietate** (rischio inaccettabile);
- il **2 agosto 2025** inizieranno ad essere sanzionate eventuali **violazioni degli obblighi per i sistemi di IA c.d. *general purpose***[10];
- il **2 agosto 2026** si assisterà alla piena efficacia dell'AI Act, con gli **obblighi per i sistemi ad alto rischio definiti nell'Allegato III**.

DISEGNO DI LEGGE 1146/2024

Anche l'Italia ha iniziato a ragionare su una possibile regolamentazione dell'IA. In particolare, il Consiglio dei ministri n. 78 del 23 aprile 2024[11] ha approvato un disegno di legge per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale (titolato "Norme per lo sviluppo e adozione di tecnologie di intelligenza artificiale")[12], in continuità con l'AI Act.

Sino al mese di marzo 2025, però, tale disegno di legge **non è stato ancora pubblicato**. Esso introduce criteri regolatori per bilanciare le opportunità delle nuove tecnologie con i rischi derivanti dal loro uso improprio, sottoutilizzo o impiego dannoso. Il testo punta a promuovere un **approccio antropocentrico**, ponendo al centro i diritti e il benessere delle persone, cercando di migliorare la qualità della vita e la coesione sociale, attraverso un'innovazione che possa definirsi responsabile. Esso interviene nei seguenti ambiti chiave:

- **strategia nazionale**: per garantire la collaborazione tra pubblico e privato, coordinando le azioni della PA in materia e le misure e gli incentivi economici rivolti allo sviluppo imprenditoriale ed industriale;

>>[8] Tuttavia, i sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'ammissione, per assegnare persone agli istituti o ai programmi di istruzione e formazione professionale a tutti i livelli, per valutare i risultati dell'apprendimento delle persone, per valutare il livello di istruzione adeguato per una persona e influenzare materialmente il livello di istruzione e formazione che le persone riceveranno o a cui potranno avere accesso o per monitorare e rilevare comportamenti vietati degli studenti durante le prove, dovrebbero essere classificati come sistemi di IA ad alto rischio, in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi può incidere sulla sua capacità di garantire il proprio sostentamento. Se progettati e utilizzati in modo inadeguato, tali sistemi possono essere particolarmente intrusivi e violare il diritto all'istruzione e alla formazione, nonché il diritto alla non discriminazione, e perpetuare modelli storici di discriminazione, ad esempio nei confronti delle donne, di talune fasce di età, delle persone con disabilità o delle persone aventi determinate origini razziali o etniche o un determinato orientamento sessuale".

[9] Art. 50.

[10] Intelligenza artificiale che può essere utilizzata per una vasta gamma di applicazioni, anziché essere progettata per un compito specifico. Sono modelli flessibili, capaci di adattarsi a diversi contesti e di svolgere molteplici funzioni, come la generazione di testo, immagini, traduzioni, analisi dati, ecc.

[11] Testo disponibile su: https://www.senato.it/leg/19/BGT/Schede/FascicoloSchedeDDL/ebook/58262.pdf

[12] Per un approfondimento: https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-78/25501

- **autorità nazionale**: per garantire il controllo e la regolamentazione dei sistemi, compiti che vengono affidati all'Agenzia per l'Italia digitale (AgID) e all'Agenzia per la cybersicurezza nazionale (ACN);
- **azioni di promozione**: per incentivare l'innovazione e la formazione in tema IA;
- **sanzioni penali**: per contrastare eventuali usi illeciti dei sistemi di IA.

LINEE GUIDA AGID E MIM

Dal 18 febbraio 2025 e fino al 20 marzo 2025 sono in consultazione pubblica le **Linee Guida per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione, adottate da AgID con la Determinazione n. 17/2025**[13].

Previste dal Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024-2026, le Linee Guida di AgID sull'adozione, l'acquisto e lo sviluppo di sistemi di IA nella Pubblica Amministrazione saranno emanate seguendo l'iter previsto all'articolo 71 del Codice dell'Amministrazione Digitale (CAD), quindi:

- vincolanti ***erga omnes***[14];
- **sanzionabili** (art. 18-bis del CAD[15]);
- **azionabili dinanzi al Giudice Amministrativo**[16].

Quelle in consultazione riguardano, nello specifico, le modalità di adozione dei sistemi di Intelligenza Artificiale, con particolare riferimento agli aspetti di conformità normativa e di impatto organizzativo.

È prevista la **futura adozione di altre Linee Guida AgID** a completamento della disciplina di settore.

Nelle Linee Guida in esame sono previsti una serie di obblighi, particolarmente stringenti per le Amministrazioni. Obblighi che rendono estremamente complessa l'**azione di adeguamento delle scuole in caso di uso di IA**. Anche perché è **mancata l'individuazione, da parte dell'IA Act, di una figura obbligatoria di monitoraggio e supporto agli enti**, come fatto dal GDPR[17] con la disciplina del *Data Protection Officer* – DPO (anche detto Responsabile per la Protezione dei Dati personali – RPD): la mancanza di un possibile "***Artificial Intelligence Officer***" aggrava ulteriormente il lavoro gestionale delle scuole e il carico di responsabilità.

Nel successivo paragrafo del presente Vademecum, dedicato alle raccomandazioni, sono riassunte le principali azioni richieste anche da AgID, con la precisazione che, ovviamente, ogni futura e concreta adozione di sistemi di IA nella scuola debba prima passare al vaglio di professionisti di settore: il DPO può coprire solo parte dell'adeguamento, quello attinente alla protezione dei dati personali. Resterebbero scoperti gli altri profili connessi all'IA Act o alle LG AgID in esame.

---

[13] Per un approfondimento: https://www.agid.gov.it/it/notizie/intelligenza-artificiale-in-consultazione-le-linee-guida-pa

[14] Nei confronti di chiunque.

[15] L'articolo in esame attribuisce ad AgID un potere sanzionatorio, azionabile sia d'ufficio che su segnalazione inviata al Difensore Civico Digitale (https://www.agid.gov.it/it/agenzia/difensore-civico-per-il-digitale), nei confronti delle Pubbliche Amministrazioni, dei gestori di pubblico servizio e delle società controllate (soggetti elencati nell'art. 2, comma 2, del CAD), in caso di violazione del CAD e delle sue Linee Guida "*e di ogni altra norma in materia di innovazione tecnologica e digitalizzazione*", con sanzioni amministrative pecuniarie comprese tra un minimo di euro 10 mila ed un massimo di euro 100 mila.

[16] Come precisato dal Consiglio di Stato nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, n. 2122 del 10 ottobre 2017.

[17] Regolamento Generale dell'UE sulla Protezione dei Dati 679/2016 (anche detto *General Data Protection Regulation* – GDPR), è la normativa dell'Unione Europea che disciplina il trattamento dei dati personali. Il quadro normativo è poi completato dal D.Lgs. 196/2003 (anche detto Codice Privacy), come modificato con il D.Lgs. 101/2018 per un suo allineamento al GDPR.

Anche il Ministero per l'Istruzione e il Merito – MIM ha annunciato l'imminente pubblicazione di Linee Guida per disciplinare un servizio digitale dedicato all'IA, che accompagnerà le scuole nell'adozione di queste tecnologie, rendendole consapevoli dei rischi e delle opportunità attraverso sistemi di verifica e monitoraggio. Si precisa, però, che tali **Linee Guida ministeriali non detengono il medesimo valore (vincolante *erga omnes*, direttamente sanzionabili e azionabili innanzi al Giudice Amministrativo) tipico invece di quelle emanate dall'AgID** ai sensi dell'art. 71 del CAD.

AUTORITÀ ISTITUENDA DI SETTORE

L'AI Act richiede agli Stati membri di indicare un'Autorità caratterizzata da requisiti di indipendenza e competenza specifici.

Con il citato Disegno di legge "Norme per lo sviluppo e adozione di tecnologie di intelligenza artificiale" (cd. DDL sull' Intelligenza Artificiale) approvato lo scorso 23 aprile e non ancora pubblicato, l'Italia ha individuato la **struttura della prossima Autorità nazionale IA, con una precisa ripartizione di compiti tra le due Agenzie componenti**:

a. **AgID**, quale responsabile della promozione dell'innovazione e dello sviluppo dell'intelligenza artificiale, nonché della definizione delle procedure e delle funzioni e compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale;
b. **ACN**, quale responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale nonché per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza.

Restano ferme le competenze, i compiti e i poteri del **Garante Privacy, nella specifica materia della protezione dei dati personali**.

FRIA E DPIA: IL NECESSARIO RISK ASSESMENT SUI DIRITTI FONDAMENTALI

Dato l'approccio antropocentrico dell'IA Act, esso prevede obblighi e adempimenti differenti in relazione al livello di rischio per i diritti e le libertà delle persone.

Per i casi di **alto livello di rischio** il Regolamento europeo introduce l'obbligo di redigere una **FRIA** (***Fundamental Rights Impact Assessment***), ossia una **valutazione d'impatto sui diritti fondamentali**, in grado di individuare preventivamente i potenziali rischi legali associati all'utilizzo di IA. In particolare, è l'art. 29 dell'AI Act ad introdurre l'obbligo per **i *deployers***, quindi anche per le **scuole che mettono in opera sistemi di IA ad alto rischio** nel loro ambiente lavorativo, di redigere, possibilmente per il tramite di una consulenza esperta di professionisti, un documento che:

a. dimostri che il sistema all'alto rischio implementato dall'organizzazione sia conforme alla legislazione nazionale ed europea sull'IA;

b. chiarisca le modalità con cui il sistema garantisce un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali dei destinatari del servizio.

Tale strumento sarà destinato a dialogare strettamente con un'altra importante valutazione che viene invece disciplinata dal GDPR, ossia la **Valutazione d'impatto sulla Protezione dei Dati (anche detta DPIA), obbligatoria non solo in caso di adozione di sistemi IA ad alto rischio**[18] **ma in qualsiasi caso di adozione di sistemi IA**.

Essa è un adempimento previsto dall'art. 35 del GDPR ed è un obbligo formale, necessario quando le attività di trattamento dei dati personali comportino dei rischi particolarmente elevati per i diritti e le libertà delle persone fisiche.

Sul punto è anche intervenuto il Garante privacy, con il **provvedimento n. 467 del 2018**[19], il quale ha previsto, ai sensi dell'art. 35 comma 4 del GDPR, **l'elenco delle tipologie di trattamenti soggetti obbligatoriamente al requisito di una valutazione d'impatto sulla protezione dei dati** tra i quali rientrano: " *i trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT;* ***sistemi di intelligenza artificiale****; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) [...]*".

In sintesi, l'eventuale integrazione di questi due documenti (FRIA e DPIA) consente di valutare globalmente i rischi associati all'utilizzo di un sistema di IA, non solo per quanto riguarda i dati personali ma anche per ciò che attiene ai diritti fondamentali potenzialmente interessati dal sistema.

SANZIONI

Come sinora delineato, **i piani normativi che disciplinano l'IA sono diversi. Quindi anche i piani sanzionatori**.

Di seguito una tabella che racchiude le **principali sanzioni amministrative pecuniarie**, permettendone una facile comprensione:

AMBITO	NORMA	ENTE SANZIONANTE	SANZIONE
Violazione norme del Codice Amministrazione Digitale o delle sue Linee Guida AgID	Art. 71 CAD Art. 18-bis CAD	AgID	Sanzione amministrativa pecuniaria tra un minimo di euro 10.000,00 e un massimo di euro 100.000,00
Violazione della normativa privacy in tema di DPIA obbligatoria	Art. 35 GDPR Provvedimento 11 ottobre 2018 del Garante Privacy[20]	Garante Privacy	Sanzione amministrativa pecuniaria sino a 10.000.000,00 di euro
Violazione del Regolamento UE n. 1689/2024 – AI Act per quanto attiene agli obblighi dei *deployer* - utilizzatori	Art. 26 AI Act Art. 99[21] AI Act	Autorità nazionale IA	Sanzione amministrativa pecuniaria fino a 15.000.000,00 di euro
Violazione del Regolamento UE n. 1689/2024 – AI Act per quanto attiene alla trasmissione di informazioni non corrette, incomplete o fuorvianti alle autorità competenti	Art. 99 AI Act	Autorità nazionale IA	Sanzione amministrativa pecuniaria fino a 7.500.000,00 di euro

[18] Espressamente prescritta in tali casi dal Considerando 96 dell'AI Act.

[19] Testo disponibile su: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9058979

[20] Si rinvia a: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9058979

[21] L'art. 99 dell'AI Act fornisce alcune indicazioni sui criteri con cui l'autorità nazionale incaricata di irrogare la sanzione dovrà valutare l'importo. Di seguito le indicazioni che maggiormente potranno attenere ››

Si ribadisce che la tabella racchiude solo le principali sanzioni amministrative pecuniarie, escludendone altre possibili. Allo stesso modo, in questa sede non si considerano le **potenziali responsabilità civili o penali**[22].

Sotto il profilo del **danno erariale**, si richiama l'attenzione sulla giurisprudenza della **Corte dei Conti che individua nel DS il soggetto responsabile** in caso di violazioni privacy che abbiano comportato una sanzione in capo all'Istituto scolastico[23]. Riteniamo che lo stesso schema logico sarà applicato dal giudice contabile anche in caso di sanzioni comminate da AgID o dall'istituenda Autorità nazionale per l'IA.

RACCOMANDAZIONI FINALI PER LE SCUOLE

In base a quanto sopra precisato appare ormai scontato come l'adozione dell'IA nelle scuole possa offrire grandi opportunità richiedendo allo stesso tempo un approccio responsabile e conforme alle normative, ormai abbastanza corpose, che delineano obblighi e adempimenti precisi anche per i meri utilizzatori dei sistemi di IA.

Le **istituzioni scolastiche**, che scelgono di implementare soluzioni di IA, **devono garantire il rispetto dei diritti fondamentali degli studenti e del personal**e, adottando misure precise per mitigare i rischi.

Di seguito, alcuni **suggerimenti pratici** al fine di rendere l'utilizzo IA in linea con l'approccio antropocentrico delineato dal legislatore europeo, garantendo un ambiente sicuro e rispettoso dei diritti e delle libertà fondamentali di studenti e destinatari finali del servizio:

- **catalogare i casi d'uso dei sistemi IA, identificando soprattutto i sistemi di IA ad alto rischio** eventualmente coinvolti nell'organizzazione e conservando a norma nel tempo la relativa documentazione;
- realizzare una **DPIA per ogni Sistema IA** da adottare, con il supporto del DPO che, quindi, abbia competenze anche in tema IA;
- realizzare una **FRIA per i soli Sistemi IA ad alto rischio**;
- assicurare la **sorveglianza umana** per i Sistemi IA ad alto rischio, tramite personale che abbia adeguate competenze;
- integrare il **Regolamento di Istituto o predisporre un Regolamento IA** *ad hoc*;
- **predisporre un'Informativa IA** a studenti e genitori;
- integrare l'**Informativa privacy generale o predisporre un'Informativa privacy** *ad hoc*;
- integrare il **Registro dei trattamenti** dei dati personali;

>>[21] a una violazione da parte di un Istituto scolastico:
- la natura, la gravità e la durata della violazione e le conseguenze tenendo in considerazione lo scopo del sistema di IA, il numero di persone coinvolte e l'entità del danno da queste subito;
- il fatturato, la quota di mercato, la dimensione del *deployer*;
- il grado di cooperazione con le autorità nazionali;
- le misure tecniche e organizzative implementate dal *deployer*;
- le modalità con cui l'autorità nazionale è venuta conoscenza della violazione;
- la volontarietà o meno della violazione;
- qualsiasi azione posta in essere dal *deployer* per mitigare l'impatto sui soggetti danneggiati.

Infine, le autorità dovranno valutare se l'importo determinato secondo i criteri illustrati sia efficace, proporzionato, dissuasivo.

[22] Il citato DDL sull'Intelligenza artificiale del 23 aprile 2024, ad es., prevede un aumento della pena per i reati commessi mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, o quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa o aggravato le conseguenze del reato.

[23] Sentenza Corte dei Conti, sez. giurisd. Lazio, n. 246/2019.

- nominare il fornitore del Sistema IA quale **Responsabile ex art. 28 GDPR**;
- valutare caso per caso la nomina del fornitore Sistema IA quale **Amministratore di sistema**;
- acquistare solo Sistemi IA in **cloud qualificato ACN**;
- approvare un **Codice etico** per l'IA;
- approvare una **Strategia interna per la PA, un Piano operativo, un Piano di comunicazione e un Piano di risposta agli incidenti di sicurezza**;
- **approvare un piano per la formazione periodica del personale** che svolge attività con il Sistema IA.

Quanto contenuto nei punti su delineati deve comunque essere ritenuto come **non esaustivo e solo indicativo, considerata l'ampiezza delle Linee Guida AgID in fase di definizione e le ulteriori possibili discipline emanabili dalle Autorità di settore, italiane ed europee**.

Per qualsiasi supporto operativo sul tema IA, noi di LiquidLaw possiamo offrire servizi di formazione e consulenza. Per i dettagli, rinviamo alla pagina dedicata alle "Scuole" del nostro sito web disponibile al seguente link:

https://www.liquidlaw.it/servizi/scuole/

All'interno della pagina web, sono descritti tutti i nostri servizi presenti sul MEPA con specifiche Offerte Dirette di Acquisto - ODA. Fermo restando la possibilità di personalizzazione (anche ai fini del DM66 o normative similari).

Di seguito le principali ODA presenti sul MEPA e sul nostro sito:

LL_FIA_SCUOLA_1	Formazione e training on the job in materia di Intelligenza artificiale nell'Istituto scolastico	euro 950,00 + IVA
LL_FAD_SCUOLA_1	Formazione e training on the job in materia di Amministrazione digitale nell'Istituto scolastico	euro 950,00 + IVA
LL_FAT_SCUOLA_1	Formazione e training on the job in materia di Amministrazione Trasparente nell'Istituto scolastico	euro 1300,00 + IVA
LL_FAP_SCUOLA_1	Formazione e training on the job in materia di Appalti e eProcurement pubblico nell'Istituto scolastico	euro 950,00 + IVA
LL_FP_SCUOLA_1	Formazione e training on the job in materia di Privacy nell'Istituto scolastico	euro 950,00 + IVA
LL_TAD_SCUOLA_1	Servizio di supporto e affiancamento in tema di Trasparenza, Amministrazione digitale e Privacy nell'Istituto scolastico per la durata di 1 anno	euro 1300,00 + IVA
LL_DPO_SCUOLA_1	Servizio DPO con affiancamento in tema di Amministrazione digitale nell'Istituto scolastico per la durata di 1 anno	euro 1080,00 + IVA
LL_DPO_SCUOLA_2	Servizio DPO con affiancamento in tema di Amministrazione digitale nell'Istituto scolastico per la durata di 2 anni	euro 2060,00 + IVA *Costo annuo:* *euro 1030,00 + IVA*
LL_DPO_SCUOLA_3	Servizio DPO con affiancamento in tema di Amministrazione digitale nell'Istituto scolastico per la durata di 3 anni	euro 2940,00 + IVA *Costo annuo:* *euro 980,00 + IVA*

www.liquidlaw.it
@liquidlawsrl
liquidlawsrl@pec.it

spin-off
UniSalento
2018-22