

AI...CHE SCUOLA!

Guida all'intelligenza artificiale per docenti curiosi

Benvenuti al corso "AI, che scuola!"

LEZIONE 2 – Normativa europea e nazionale sull'uso dell'AI

Durata: 60 minuti

INTRODUZIONE

Benvenuti alla seconda lezione del nostro percorso sull'intelligenza artificiale nella scuola. Oggi affrontiamo un tema che può sembrare arido ma è assolutamente fondamentale: il quadro normativo che regola l'uso dell'AI, in particolare nel contesto educativo.

Perché è così importante? Perché come docenti non siamo solo educatori, siamo anche pubblici ufficiali con responsabilità precise. Ogni volta che usiamo uno strumento digitale con i nostri studenti, ogni volta che inseriamo dati in un sistema, ogni volta che prendiamo decisioni che coinvolgono tecnologie, ci muoviamo in un campo regolato da norme specifiche. Non conoscerle non ci esonera dal rispettarle.

Ma la normativa non è solo un vincolo: è anche una protezione per noi, per gli studenti, per le famiglie. Ci aiuta a navigare in sicurezza un territorio nuovo e complesso.

1. AI ACT EUROPEO: PRINCIPI E APPROCCIO PER RISCHIO

L'Unione Europea ha approvato nel 2024 l'AI Act, il primo regolamento organico al mondo sull'intelligenza artificiale. È entrato in vigore progressivamente e rappresenta la cornice normativa di riferimento per tutti gli Stati membri.

Obiettivi fondamentali dell'AI Act

Il regolamento si basa su tre pilastri:

- Proteggere i diritti fondamentali dei cittadini europei
- Garantire la sicurezza e la trasparenza dei sistemi di AI
- Promuovere l'innovazione responsabile e la competitività europea

Non è quindi un regolamento "contro" l'AI, ma un tentativo di governarla in modo che rispetti i valori europei: dignità umana, democrazia, stato di diritto, diritti fondamentali.

L'approccio basato sul rischio

La grande innovazione dell'AI Act è l'approccio risk-based. Non tutte le AI sono regolate allo stesso modo, ma in base al rischio che rappresentano per i diritti e la sicurezza delle persone.

Il regolamento identifica quattro categorie:

Rischio inaccettabile - Sistemi vietati completamente. Includono il social scoring da parte delle autorità pubbliche (come in alcuni paesi viene assegnato un punteggio sociale ai cittadini), la manipolazione subliminale che può causare danni, lo sfruttamento delle vulnerabilità di gruppi specifici, e alcuni sistemi di identificazione biometrica in tempo reale in spazi pubblici. Questi sistemi sono considerati incompatibili con i valori europei.

Rischio alto - Sistemi che devono rispettare requisiti stringenti prima di essere immessi sul mercato. Vedremo tra poco che l'educazione rientra in questa categoria. Questi sistemi devono garantire trasparenza, sicurezza, supervisione umana, robustezza tecnica, accuratezza.

Rischio limitato - Sistemi soggetti principalmente a obblighi di trasparenza. Ad esempio, i chatbot devono dichiarare di essere AI, i contenuti generati (deepfake, audio sintetici) devono essere etichettati come tali. Gli utenti hanno il diritto di sapere quando interagiscono con un sistema automatico.

Rischio minimo - La maggior parte delle applicazioni AI, come filtri antispam, videogiochi con AI, sistemi di raccomandazione base. Nessun obbligo particolare, ma restano valide le normative generali sulla protezione dei consumatori e dei dati.

Principi trasversali

Indipendentemente dal livello di rischio, l'AI Act stabilisce alcuni principi generali che devono guidare lo sviluppo e l'uso dell'AI: supervisione umana (human oversight), nessuna decisione completamente automatizzata su questioni significative, trasparenza sul funzionamento dei sistemi, accountability (qualcuno deve essere responsabile), protezione dei dati personali, non discriminazione e fairness.

2. SISTEMI AD ALTO RISCHIO E IMPLICAZIONI SCOLASTICHE

Ecco il punto cruciale per noi: l'AI Act classifica esplicitamente i sistemi di AI utilizzati nell'istruzione e nella formazione come sistemi ad alto rischio.

Perché l'educazione è considerata ad alto rischio?

L'educazione è un ambito fondamentale per lo sviluppo della persona e per l'accesso alle opportunità. Un sistema di AI che influenza percorsi educativi, valutazioni, orientamento può avere un impatto profondo e duraturo sulla vita degli studenti. Può determinare chi accede a certe opportunità, chi viene etichettato come "bravo" o "in difficoltà", chi viene indirizzato verso certi percorsi piuttosto che altri.

Per questo motivo, l'AI Act richiede che i sistemi AI usati per:

- Determinare l'accesso a istituzioni educative
- Valutare gli studenti
- Monitorare e rilevare comportamenti scorretti (ad esempio, sistemi anti-plagio avanzati)
- Orientare gli studenti verso percorsi formativi specifici

debbano rispettare requisiti molto stringenti.

Cosa significa per le scuole?

Prima di tutto, dobbiamo distinguere tra fornitori e utenti di sistemi AI. I fornitori (le aziende che sviluppano i sistemi) hanno l'obbligo di garantire conformità tecnica, documentazione, test di

accuratezza, sistemi di gestione del rischio. Le scuole, in quanto utenti, hanno responsabilità diverse ma ugualmente importanti.

Come utilizzatori, le scuole devono:

- Verificare che i sistemi AI acquistati o utilizzati siano conformi all'AI Act
- Garantire che ci sia sempre supervisione umana adeguata
- Monitorare il funzionamento dei sistemi e segnalare malfunzionamenti
- Formare il personale sull'uso corretto
- Informare studenti e famiglie sull'uso di sistemi AI

Esempi concreti per il contesto scolastico

Facciamo chiarezza con esempi pratici. Un sistema che analizza automaticamente i compiti scritti e propone voti rientra nella categoria ad alto rischio, perché influenza direttamente la valutazione. Un software che traccia il comportamento degli studenti online per identificare rischi di abbandono scolastico è ad alto rischio. Una piattaforma che suggerisce percorsi di orientamento basandosi su algoritmi è ad alto rischio.

Invece, un semplice chatbot che risponde a domande generali su un argomento di studio, usato come supporto didattico senza impatto sulla valutazione, non rientra automaticamente nella categoria ad alto rischio. Un sistema di correzione ortografica potenziato dall'AI è a rischio minimo. La differenza sta nell'impatto sulle decisioni significative riguardanti gli studenti.

Il principio della supervisione umana

Questo è forse l'aspetto più importante per i docenti: nessun sistema AI può prendere decisioni significative in completa autonomia. Ci deve sempre essere un essere umano che comprende il funzionamento del sistema, che può intervenire, che valuta criticamente i risultati, che ha l'autorità di disattivare o ignorare il sistema se necessario. Il docente non può delegare il proprio giudizio professionale a un algoritmo.

3. GDPR: TRATTAMENTO DEI DATI

Prima ancora dell'AI Act, esiste dal 2018 il GDPR (General Data Protection Regulation), il regolamento europeo sulla protezione dei dati personali. Ogni volta che usiamo un sistema AI con dati degli studenti, il GDPR si applica.

Principi fondamentali del GDPR

Il GDPR si basa su alcuni principi che dobbiamo sempre tenere a mente:

Liceità, correttezza e trasparenza - I dati devono essere trattati in modo legale, giusto e trasparente. Gli interessati (studenti e famiglie) devono sapere cosa facciamo con i loro dati.

Limitazione della finalità - I dati possono essere raccolti solo per scopi specifici, espliciti e legittimi. Non posso raccogliere dati "per ogni evenienza" o usarli per scopi diversi da quelli dichiarati.

Minimizzazione dei dati - Devo raccogliere solo i dati strettamente necessari per la finalità dichiarata. Questo è particolarmente importante con l'AI, che spesso "chiede" molti dati.

Esattezza - I dati devono essere accurati e aggiornati. Dati errati possono portare a decisioni sbagliate, soprattutto se elaborati da AI.

Limitazione della conservazione - I dati non possono essere conservati indefinitamente, ma solo per il tempo necessario.

Integrità e riservatezza - I dati devono essere protetti da accessi non autorizzati, perdite, distruzioni.

Accountability - Chi tratta i dati deve essere in grado di dimostrare la conformità al GDPR.

Base giuridica per il trattamento

Quando usiamo un sistema AI con dati degli studenti, dobbiamo avere una base giuridica. Nel contesto scolastico, le basi più comuni sono:

- **Obbligo legale:** trattamenti necessari per adempiere obblighi previsti dalla legge (ad esempio, registri elettronici).
- **Esecuzione di un compito di interesse pubblico:** la scuola svolge una funzione pubblica e può trattare dati necessari per questa funzione.
- **Consenso:** in alcuni casi specifici, può essere necessario il consenso esplicito (informato, libero, specifico, revocabile).

È importante capire che nella scuola pubblica il consenso è raramente la base giuridica corretta, perché non è veramente "libero" quando si tratta di attività scolastiche ordinarie. Tuttavia, per attività facoltative o sperimentali, il consenso può essere necessario.

Informativa e diritti degli interessati

Prima di usare un sistema AI con dati degli studenti, dobbiamo fornire un'informativa chiara che spieghi: quali dati raccogliamo, per quale finalità, su quale base giuridica, per quanto tempo li conserviamo, chi può accedervi, se vengono trasferiti fuori dall'UE, quali diritti hanno gli interessati.

Gli studenti (o i loro genitori se minorenni) hanno diritti specifici: accesso ai propri dati, rettifica di dati errati, cancellazione in certi casi, limitazione del trattamento, opposizione, portabilità dei dati. E soprattutto, il diritto di non essere sottoposti a decisioni basate unicamente su trattamenti automatizzati che producono effetti significativi.

4. DATI PERSONALI VS DATI SENSIBILI

È fondamentale capire la differenza perché le protezioni richieste sono diverse.

Dati personali

Sono tutte le informazioni che permettono di identificare una persona fisica: nome, cognome, codice fiscale, indirizzo email, numero di telefono, fotografia, indirizzo IP, identificativi online. Nel contesto scolastico: nome dello studente, classe, voti, assenze, note disciplinari, elaborati scolastici firmati.

Categorie particolari di dati (ex dati sensibili)

Il GDPR li chiama "categorie particolari" e richiedono protezioni rafforzate. Includono dati che rivelano: origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche,

appartenenza sindacale, dati genetici, dati biometrici (quando usati per identificare univocamente una persona), dati relativi alla salute, dati relativi alla vita sessuale o all'orientamento sessuale.

Nel contesto scolastico sono dati sensibili: certificazioni di disabilità, diagnosi di DSA o BES, informazioni su situazioni familiari difficili (affidi, tutele), dati sanitari in generale, religione dichiarata per l'insegnamento dell'ora alternativa, dati biometrici per controllo accessi.

Perché questa distinzione è importante con l'AI?

Perché alcuni sistemi di AI, per funzionare, potrebbero richiedere o elaborare dati sensibili anche indirettamente. Ad esempio, un sistema che analizza i testi degli studenti potrebbe inferire informazioni sulla salute mentale, sulle convinzioni religiose, sull'orientamento sessuale. Un sistema di riconoscimento facciale tratta dati biometrici. Un sistema di personalizzazione dell'apprendimento potrebbe usare informazioni su disabilità o disturbi specifici.

Per i dati sensibili, le regole sono più stringenti: servono garanzie aggiuntive, spesso è necessaria una valutazione d'impatto sulla protezione dei dati (DPIA), la base giuridica deve essere ancora più solida.

Regola pratica per i docenti

Quando considerate di usare un sistema AI, chiedetevi sempre: quali dati degli studenti entreranno in questo sistema? Sono solo dati personali comuni o anche categorie particolari? Questi dati sono davvero necessari o posso raggiungere lo stesso obiettivo con meno dati o con dati anonimizzati? Dove finiscono questi dati? Quanto tempo restano nel sistema?

5. RESPONSABILITÀ DEL DOCENTE

Parliamo ora di un tema delicato ma essenziale: la responsabilità personale del docente nell'uso dell'AI.

Responsabilità professionale

Come docenti, abbiamo una responsabilità professionale che deriva dalla nostra funzione educativa. Siamo responsabili delle scelte didattiche che facciamo, degli strumenti che utilizziamo, dell'impatto che queste scelte hanno sugli studenti. Questa responsabilità non viene meno quando usiamo l'AI, anzi, si amplifica perché stiamo usando strumenti potenti e non sempre trasparenti.

Non possiamo dire "l'AI mi ha dato questo risultato quindi l'ho usato". Dobbiamo essere in grado di valutare criticamente i risultati, di comprendere i limiti dello strumento, di intervenire quando necessario. Se un sistema di AI propone una valutazione ingiusta, se genera contenuti inappropriati, se commette errori, la responsabilità finale è nostra.

Responsabilità amministrativa

Lavorando nella scuola pubblica, siamo dipendenti pubblici. Questo comporta obblighi specifici: rispettare le direttive dell'amministrazione, seguire le procedure stabilite, documentare le nostre scelte. Se la scuola ha adottato policy sull'uso dell'AI, dobbiamo conoscerle e rispettarle. Se usiamo sistemi non autorizzati o in modo non conforme, possiamo incorrere in responsabilità amministrative.

Responsabilità civile e penale

In casi estremi, possono configurarsi anche responsabilità civili o penali. Ad esempio, se per negligenza nell'uso di un sistema AI causiamo un danno a uno studente (violazione della privacy, discriminazione, danno psicologico), potremmo essere chiamati a rispondere civilmente. Se violiamo gravemente il GDPR, sono previste sanzioni anche penali in certi casi. Non voglio allarmarvi, questi casi estremi sono rari. Ma è importante essere consapevoli che la responsabilità esiste e che "non lo sapevo" o "ho fatto come gli altri" non sono difese valide.

Responsabilità collegiale

C'è anche una dimensione collegiale. Le decisioni sull'uso di sistemi AI che impattano sulla didattica, sulla valutazione, sull'organizzazione scolastica dovrebbero essere prese collegialmente, discusse, condivise. Il Collegio Docenti, i Dipartimenti, i Consigli di Classe sono sedi appropriate per queste discussioni. L'uso dell'AI non dovrebbe essere una scelta individuale e isolata, ma parte di un progetto educativo condiviso.

La figura del DPO

Ogni scuola ha (o dovrebbe avere) un Data Protection Officer (DPO), il Responsabile della Protezione dei Dati. È la figura di riferimento per tutte le questioni legate al GDPR. Prima di adottare un nuovo sistema AI, dovremmo consultare il DPO per verificare la conformità normativa. Il DPO non è un ostacolo burocratico, ma un alleato che ci protegge da errori potenzialmente gravi.

6. NOTA DEL MIM SULL'USO DELL'AI

Il Ministero dell'Istruzione e del Merito ha emanato nel 2023 una nota specifica sull'uso dell'intelligenza artificiale nella scuola. Vediamo i punti salienti.

Contesto e obiettivi della nota

La nota ministeriale riconosce che l'AI è già entrata nelle scuole e che vietarla non è né possibile né auspicabile. L'obiettivo è fornire un quadro di riferimento per un uso consapevole, responsabile e pedagogicamente fondato.

Il documento si inserisce nella cornice europea (AI Act, GDPR) e nelle indicazioni nazionali sul Piano Nazionale Scuola Digitale e sulle competenze digitali dei cittadini.

Principi guida indicati dal MIM

La nota ministeriale stabilisce alcuni principi fondamentali:

Centralità della persona e della relazione educativa - L'AI deve essere al servizio dell'apprendimento e della relazione educativa, non sostituirla. Il docente resta il regista del processo educativo.

Trasparenza e consapevolezza - Studenti e famiglie devono essere informati quando e come viene usata l'AI. Non ci possono essere usi "nascosti" o non dichiarati.

Protezione dei dati e della privacy - Particolare attenzione alla tutela dei dati personali degli studenti, con richiamo esplicito al GDPR e alle cautele necessarie.

Sviluppo del pensiero critico - L'AI deve essere anche oggetto di studio ed educazione critica, non solo strumento d'uso.

Equità e inclusione - L'AI non deve amplificare disuguaglianze o discriminazioni, ma deve essere usata per promuovere inclusione e personalizzazione positiva.

Indicazioni operative

Il MIM suggerisce alle scuole di:

- Costituire gruppi di lavoro sull'AI che coinvolgano docenti, dirigenti, eventualmente studenti e genitori
- Elaborare policy interne sull'uso dell'AI, chiare e condivise
- Prevedere momenti di formazione per il personale scolastico
- Integrare l'educazione all'AI nei curricula, in particolare nell'educazione civica digitale
- Documentare e condividere buone pratiche
- Valutare periodicamente l'impatto dell'uso dell'AI sulla didattica e sul benessere degli studenti

Valutazione e AI

Un punto specifico riguarda la valutazione. Il MIM chiarisce che l'AI può essere usata come supporto nella correzione e nella preparazione di verifiche, ma la valutazione finale deve sempre essere un atto professionale del docente, basato su giudizio umano, che considera il percorso complessivo dello studente, non solo il prodotto finale.

Si raccomanda inoltre di ripensare le modalità di verifica in un contesto in cui gli studenti hanno accesso all'AI: privilegiare compiti autentici, valutare i processi oltre ai prodotti, usare verifiche orali e pratiche, chiedere agli studenti di documentare il loro percorso di lavoro.

7. BUONE PRATICHE LEGALI PER LA SCUOLA

Traduciamo ora tutto questo in azioni concrete. Cosa dovremmo fare per usare l'AI nella legalità e nella sicurezza?

Prima di adottare un sistema AI

Valutazione preliminare - Chiedetevi: è davvero necessario? Quali benefici porta? Quali rischi comporta? Esistono alternative meno problematiche?

Verifica della conformità - Controllate che il fornitore sia in regola con AI Act e GDPR. Leggete le condizioni d'uso, l'informativa privacy, le policy del servizio. Verificate dove sono conservati i dati (se fuori dall'UE, ci devono essere garanzie adeguate).

Consultazione del DPO - Non saltate questo passaggio. Il DPO può segnalare criticità che voi non vedete e suggerire soluzioni.

Approvazione collegiale - Se l'uso dell'AI impatta su più classi o su aspetti significativi della didattica, portatelo in Collegio Docenti o almeno in Consiglio di Classe per una decisione condivisa.

Durante l'uso

Informativa agli studenti e alle famiglie - Spiegate chiaramente quando e come usate l'AI, per quali scopi, con quali dati. Potete farlo in una circolare, in una riunione, attraverso il sito della scuola. La trasparenza è protezione per tutti.

Conservazione minima dei dati - Non chiedete o non inserite dati che non servono. Se un sistema chiede troppi dati, valutate se è davvero quello giusto. Cancellate i dati quando non servono più.

Supervisione costante - Non lasciate che l'AI lavori in autonomia. Controllate i risultati, verificate che non ci siano errori o bias, intervenite se necessario.

Documentazione - Tenete traccia di come usate l'AI: per quale attività, con quali studenti, con quali risultati, quali problemi avete incontrato. Questa documentazione può essere preziosa sia per migliorare le pratiche sia, in caso di contestazioni, per dimostrare la vostra diligenza.

Dopo l'uso

Valutazione d'impatto - Periodicamente, fermatevi a riflettere: l'uso dell'AI ha portato i benefici attesi? Ci sono stati problemi? Gli studenti e le famiglie come hanno reagito? Cosa cambieremmo?

Aggiornamento - Le normative, le tecnologie, le buone pratiche evolvono. Quello che è conforme oggi potrebbe non esserlo domani. Rimanete aggiornati, partecipate a formazioni, leggete le circolari ministeriali.

Condivisione - Se avete trovato un buon modo di usare l'AI rispettando le norme, condividetelo con i colleghi. Le buone pratiche si diffondono per contagio positivo.

8. ERRORI COMUNI DA EVITARE

Concludiamo con una carrellata degli errori più frequenti che abbiamo osservato nell'uso dell'AI a scuola. Conoscerli vi aiuterà a evitarli.

Errore 1: Usare servizi AI gratuiti senza leggere le condizioni

Molti docenti usano ChatGPT, Gemini, o altri servizi nella versione gratuita, inserendo dati degli studenti senza rendersi conto che le condizioni d'uso di questi servizi spesso prevedono che i dati possano essere usati per addestrare il modello. Risultato: i dati degli studenti finiscono in un database dell'azienda, violando il GDPR.

Soluzione: usate solo versioni educational o aziendali di questi servizi, che offrono garanzie sulla protezione dei dati, oppure anonimizzate completamente i dati prima di inserirli (niente nomi, niente dati identificativi).

Errore 2: Far usare l'AI agli studenti senza informativa

Alcuni docenti chiedono agli studenti di usare ChatGPT o altri strumenti per compiti a casa, senza aver informato le famiglie, senza aver verificato le condizioni d'uso, senza fornire indicazioni chiare. Gli studenti creano account, inseriscono dati personali, accettano condizioni che non capiscono.

Soluzione: se volete che gli studenti usino uno strumento AI, prima verificate voi le condizioni, preparate un'informativa per le famiglie, fornite linee guida chiare agli studenti, assicuratevi che l'uso sia sicuro e conforme.

Errore 3: Delegare la valutazione all'AI

Alcuni docenti usano sistemi AI per correggere compiti e assegnare voti, accettando acriticamente i risultati. Questo viola il principio della supervisione umana e può portare a valutazioni ingiuste.

Soluzione: l'AI può essere un supporto (ad esempio, segnalare possibili errori, suggerire aree di miglioramento), ma la valutazione finale è sempre del docente, basata sul suo giudizio professionale che considera il contesto, il percorso dello studente, elementi che l'AI non può cogliere.

Errore 4: Non considerare i bias dell'AI

L'AI può perpetuare stereotipi e discriminazioni presenti nei dati di addestramento. Un docente che usa acriticamente contenuti generati dall'AI (testi, immagini, esempi) può trasmettere bias senza rendersene conto.

Soluzione: verificate sempre i contenuti generati dall'AI. Chiedetevi: ci sono stereotipi di genere, culturali, etnici? Le rappresentazioni sono equilibrate? Le fonti sono affidabili? Integrate con la vostra conoscenza e il vostro giudizio critico.

Errore 5: Non coinvolgere il dirigente scolastico

Alcuni docenti iniziano a usare sistemi AI su propria iniziativa, senza informare il dirigente, senza verificare se ci sono policy della scuola, senza chiedere autorizzazioni necessarie.

Soluzione: il dirigente è il titolare del trattamento dei dati nella scuola e ha responsabilità legali precise. Informate sempre il dirigente delle vostre intenzioni, chiedete se ci sono linee guida da seguire, collaborate per definire modalità sicure.

Errore 6: Conservare dati più a lungo del necessario

Alcuni sistemi AI conservano cronologie, chat, elaborati per periodi indefiniti. Se non facciamo attenzione, dati degli studenti restano nei server per mesi o anni oltre il necessario.

Soluzione: verificate le policy di conservazione dei dati del servizio che usate. Cancellate periodicamente dati non più necessari. Se il servizio non permette cancellazione, valutate se è quello giusto.

Errore 7: Ignorare le segnalazioni di studenti o famiglie

A volte studenti o famiglie esprimono preoccupazioni sull'uso dell'AI: timori sulla privacy, disagio nell'usare certi strumenti, richieste di spiegazioni. Alcuni docenti minimizzano o ignorano queste segnalazioni.

Soluzione: prendete sul serio ogni segnalazione. Ascoltate, spiegate, se necessario modificate l'approccio. La fiducia di studenti e famiglie è fondamentale e va costruita con trasparenza e rispetto.

Errore 8: Pensare "tanto lo fanno tutti"

La diffusione di una pratica non la rende automaticamente legale o giusta. Il fatto che molti colleghi usino un certo strumento in un certo modo non significa che sia conforme alle norme. Soluzione: verificate sempre in prima persona. Basatevi su fonti autorevoli (normative, indicazioni ministeriali, pareri del DPO), non sul "sentito dire" o sulle abitudini diffuse.

CONCLUSIONE

Lo so, questa lezione è stata densa di norme, regole, caveat. Potrebbe sembrare che la normativa sia un ostacolo all'innovazione, un insieme di paletti che limitano la nostra libertà di insegnamento.

Vi invito a ribaltare la prospettiva. La normativa è uno strumento che ci protegge e che protegge i nostri studenti. È il frutto di una riflessione profonda su quali valori vogliamo difendere in una società sempre più tecnologica: la dignità della persona, la privacy, la non discriminazione, la trasparenza, la responsabilità.

Quando rispettiamo queste norme, non stiamo solo evitando sanzioni, stiamo agendo coerentemente con la nostra missione educativa. Stiamo dicendo ai nostri studenti: "La tecnologia è potente, ma è al servizio dell'essere umano, non viceversa. I vostri diritti contano. La vostra privacy conta. Il giudizio umano conta."

Le norme sembrano complicate, ma si riassumono in alcuni principi semplici: trasparenza (dite sempre cosa fate e perché), protezione dei dati (usate solo quelli necessari e proteggerli), supervisione umana (non delegate decisioni importanti alle macchine), responsabilità (siate sempre consapevoli delle conseguenze delle vostre scelte).

Nella prossima lezione entreremo nel pratico: vedremo quali strumenti di AI esistono, come funzionano, come usarli concretamente nella didattica rispettando il quadro normativo che abbiamo costruito oggi.

Ricordate: non siete soli in questo percorso. Avete il DPO, il dirigente, i colleghi, le risorse ministeriali. E soprattutto, avete il vostro buon senso professionale e la vostra attenzione al benessere degli studenti. Se partite da lì, difficilmente sbaglierete strada.