Terre rare: una start up inglese ne riduce la dipendenza con l'IA

Terre rare per magneti mai più? La startup britannica Materials Nexus è uscita sul mercato con una innovazione resa possibile attraverso l'uso di una piattaforma di Intelligenza Artificiale (IA) che ha esplorato sistematicamente un vasto database di materiali per identificare combinazioni ottimali che sostituiscano le attuali tecnologie arrivando in soli tre mesi ad un risultato promettente, un tempo significativamente inferiore rispetto ai decenni necessari con i metodi tradizionali. La rilevanza di MagNex si estende al di là della sua rapidità di sviluppo; rappresenta una svolta potenziale per l'industria dei motori elettrici e altre tecnologie dipendenti dai magneti. Tradizionalmente, questi dispositivi si affidano alle terre rare, che, nonostante il loro nome, sono abbondanti ma complesse e costose da estrarre. Inoltre, la produzione di terre rare è geograficamente concentrata e spesso associata a problemi geopolitici e ambientali, specialmente in Cina, che detiene oltre l'80% del mercato.
Il contesto più ampio del testo è la corsa globale verso la transizione energetica e la riduzione della dipendenza dai materiali problematici come le terre rare. In questo scenario, l'innovazione non solo promette di rendere la produzione di motori elettrici più sostenibile ma anche più economica, riducendo i costi dei materiali fino all'80% e le emissioni di CO2 del 70% rispetto ai magneti tradizionali. Oltre ai motori elettrici, i magneti permanenti trovano applicazione in una varietà di tecnologie, come turbine eoliche, dispositivi medici di imaging, memorie informatiche e sistemi audio. Pertanto, MagNex ha il potenziale per influenzare positivamente diverse industrie, contribuendo significativamente alla diffusione di tecnologie sostenibili e accelerando la transizione verso un futuro a basso tenore di carbonio. Il successo di questa iniziativa suggerisce che l'approccio basato sull'IA potrebbe essere esteso ad altre aree spianando la strada a ulteriori innovazioni nei materiali strategici.

C.G.

APOSTOLATO DIGITALE

condividere codici di salvezza

ANALISI/2 – IL FUTURO DELL'ISTRUZIONE SI STA ORIENTANDO VERSO UN MODELLO «IBRIDO»

La didattica digitale per un apprendimento più flessibile e inclusivo

Sempre più si ritiene fondamentale il ruolo di un apprendimento basato non solo sui nostri sensi, in cui l'aspetto emozionale sia protagonista. Rendere accattivante e dinamica una lezione (di per sé noiosa) stimola tutti i canali di apprendimento e aumenta la partecipazione e la collaborazione tra gli studenti.
Il futuro dell'istruzione sembra essere sempre più orientato verso un modello ibrido, che combina lezioni tradizionali e digitali. Tale approccio può sfruttare i punti di forza di entrambe le metodologie, creando un ambiente di apprendimento più flessibile e inclusivo. Il successo risiede nella capacità di adattarsi e innovare, alla costante ricerca di nuove soluzioni per migliorare l'esperienza educativa e preparare gli studenti alle sfide della modernità.
Non dobbiamo dimenticarci che il divario generazionale tra docenti e studenti è ampio: oggi abbiamo insegnanti della cosiddetta generazione X che parlano ad alunni della generazione Alpha, due mondi diametralmente opposti. Per comunicare è tuttavia necessario creare dei ponti e lo sforzo maggiore deve essere svolto dal docente. Occorre sradicarsi dalle granitiche sicurezze e avventurarsi nell'esplorazione del «continente digitale», al fine di non avere «abitanti» che crescono pensando che l'IA sia il loro libro di testo e senza sapere che la stessa Intelligenza Artificiale «impara».
Il percorso dell'apprendimento è stato, è e sarà sempre mediato da contenuti analogici o tradizionali inseriti in processi di rielaborazione digitale.
L'introduzione dell'Intelligenza Artificiale nelle tecnologie didattiche è stato un ulteriore passo in avanti, ma il terreno rischia di essere ancora piuttosto accidentato e pericoloso se affrontato senza consapevolezza, in primis da parte dei docenti. Lo strumento è sì potente, ma ciò che ci restituisce non è sempre affidabile: proprio tale aspetto potrebbe essere una leva per sviluppare il senso critico negli studenti.
Ho deciso di usare solo alcune delle possibilità date dall'IA. L'esperimento più riuscito è stata la creazione di una chatbot nel quale la stessa IA impersonificava un matematico che dialogava con gli alunni spiegando i suoi teoremi. È suggestivo assistere, seppur virtualmente, al dialogo tra uno studente di oggi e Pitagora. La tecnologia crea un ponte meraviglioso e permette inoltre di valutare anche la capacità di porre domande e di rispondere alle argomentazioni avanzate dalla chatbot.
Passando da una verifica tradizionale alla risoluzione di una Escape Room con quesiti geometrici (che nella tradizione erano le domande), ho aperto il mondo della geometria ai miei alunni: sono «costretti» ad acquisire delle conoscenze per poter proseguire nella risoluzione del gioco, ma mettono in campo altre capacità, non limitandosi all'arida ripetizione di concetti avulsi da un contesto. Quando arrivano a chiedere di ripetere il percorso, si ottiene la cartina di tornasole che il procedimento adottato funziona. Non è semplice creare una Escape Room; tuttavia, se si realizza un prodotto originale, il risultato può veramente costruirsi sul processo di apprendimento svolto in classe. L'aspetto grafico accattivante, lo stimolo fornito da un traguardo raggiunto, la possibilità di personalizzare i personaggi in base agli interessi sono caratteristiche incredibili con cui un libro di testo non regge il confronto.
È essenziale affrontare le sfide legate a questa transizione, fornendo una formazione adeguata agli insegnanti e garantendo l'accesso equo alle risorse tecnologiche agli studenti. La didattica digitale è più di una semplice tendenza: è una trasformazione in grado di ridefinire il concetto stesso di processo educativo. Con il giusto supporto e una visione lungimirante, potrà continuare a crescere e prosperare, offrendo opportunità straordinarie agli educatori e agli alunni di tutto il mondo.
Don Bosco, nella sua saggezza pedagogica, diceva che bisogna «amare quello che amano i giovani» e chissà che questo orizzonte tecnologico non possa essere una modalità per veicolare, in modo originale, un po' di quell'amore verso lo studio spesso latente negli studenti di oggi abituati all'immediatezza e poco avvezzi ad uno sforzo che richiede costanza.

Elena CRISTINO
docente Scuola Valsalice
(2.fine)

Apostolato digitale
ospite a TG Piemonte

GLOSSARIO/28 – FURTI SULLE RETI

Dati in transito, come difendersi dallo «sniffing»

Lo sniffing è una pratica utilizzata per intercettare e analizzare il traffico di dati in una rete. Questa tecnica viene spesso impiegata dagli amministratori per monitorare e risolvere problemi, ma è anche sfruttata da malintenzionati per sottrarre informazioni sensibili. Lo sniffing avviene attraverso l'uso di strumenti chiamati sniffer, che sono software o hardware progettati per catturare e analizzare pacchetti di dati in transito tra dispositivi in una rete. Quando uno sniffer intercetta questi pacchetti, può esaminarne il contenuto per estrarre informazioni come credenziali di accesso, email, conversazioni e altri dati personali o aziendali.
In una rete non crittografata, i dati possono essere letti in chiaro, rendendo lo sniffing una minaccia significativa per la sicurezza. Esistono due principali tipi di sniffing: quello

passivo e quello attivo. Lo sniffing passivo consiste nel monitorare il traffico di rete senza influenzarlo in alcun modo. Questa tecnica è più difficile da rilevare poiché non altera il normale funzionamento della rete. D'altra parte, lo sniffing attivo comporta l'invio di pacchetti di dati falsi o modificati nella rete per ingannare i dispositivi e ottenere informazioni. Questo tipo di sniffing è più invasivo e può causare interruzioni nel funzionamento della rete, rendendolo più facile da individuare. Per proteggere una rete dallo sniffing, è importante implementare misure di sicurezza come la crittografia dei dati, l'uso di reti virtuali private (VPN), e l'adozione di protocolli di sicurezza come HTTPS e SSL/TLS. Inoltre, è fondamentale mantenere aggiornati i software di rete e monitorare regolarmente il traffico per rilevare eventuali attività sospette. L'educazione degli utenti su pratiche di sicurezza, come l'uso di password forti e la consapevolezza delle minacce informatiche, è altrettanto importante per prevenire attacchi di sniffing.