L'AI tra etica e sicurezza: quale futuro per le aziende?



L'adozione dell'Intelligenza Artificiale (AI) nelle aziende apre nuove opportunità, ma richiede un approccio responsabile per mitigare i rischi legati alla sicurezza dei dati, alle decisioni automatizzate e alle implicazioni etiche.

Pietro Vassalli,
responsabile Cyber Security di Gruppo Sicurezza

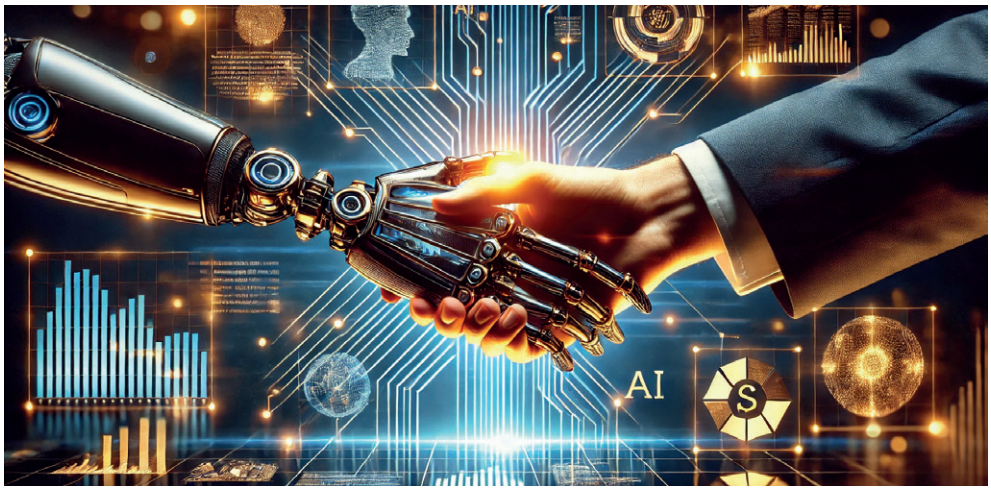
Misure di protezione avanzate e indicazioni chiare ai collaboratori sono essenziali per garantire uno sviluppo sostenibile e sicuro.

L'intelligenza artificiale sta rivoluzionando il mondo del lavoro, ma con questa trasformazione emergono nuove sfide, soprattutto in termini di sicurezza. Quali sono le principali preoccupazioni da affrontare?

L'AI sta trasformando il modo in cui lavoriamo e gestiamo le informazioni. Non mancano però i rischi. Il problema più urgente riguarda la protezione dei dati: le aziende si trovano a elaborare enormi quantità di informazioni, spesso sensibili. È importante capire come queste informazioni si inseriscano in questa tecnologia: se l'implementazione non è gestita correttamente può diventare un bersaglio per attacchi informatici, può essere utilizzata in modo improprio o può esporre informazioni riservate. Pensiamo, ad esempio, a un sistema di AI che analizza dati finanziari: se non protetto adeguatamente, potrebbe esporre dati critici con conseguenze disastrose. Il vero nodo è trovare un equilibrio tra innovazione e sicurezza, garantendo trasparenza nei processi decisionali.

Uno degli aspetti più critici riguarda il fatto che l'AI prende sempre più decisioni in autonomia. Affidarsi completamente a questi sistemi può essere rischioso?

L'automazione è straordinaria quando funziona bene, ma può diventare un problema in assenza di un adeguato controllo umano. Pensiamo alla selezione del personale: se



un algoritmo viene addestrato su dati storici distorti, rischia di perpetuare discriminazioni senza che nessuno se ne accorga. Lo stesso vale per l'assegnazione di prestiti bancari o per la valutazione dei rischi in ambito sanitario. L'AI deve essere uno strumento di supporto, non un sostituto del giudizio umano. Il rischio più grande è quello di delegare troppo, dimenticando che un algoritmo non ha un'etica propria, ma riflette quella di chi lo ha creato.

In diversi settori, l'adozione dell'AI sta già facendo una grande differenza. Quali sono quelli in cui il suo impatto è più evidente e in che misura sta cambiando le dinamiche lavorative?

Il settore medico, ad esempio, sta beneficiando enormemente dell'intelligenza artificiale per la diagnosi precoce di malattie. Tuttavia, per quanto possa essere precisa, l'AI non può sostituire il medico, ma solo affiancarlo. Lo stesso vale per il settore legale, dove gli algoritmi analizzano contratti e sentenze, o per la sicurezza informatica, dove le AI riconoscono e prevengono attacchi informatici. Ma c'è un punto fondamentale: in tutti questi settori, il controllo umano è imprescindibile. Una macchina può segnalare una possibile anomalia, ma solo un esperto può interpretarla correttamente.

Tuttavia, l'uso di algoritmi avanzati solleva anche questioni etiche, come il rischio di bias nelle decisioni automatizzate. Come possiamo prevenire discriminazioni e garantire equità?

Fino ad oggi, il bias negli algoritmi è stato un problema reale: l'AI ha imparato dai dati storici, che spesso riflettono pregiudizi inconsapevoli. Per questo, se in passato le assunzioni nelle aziende hanno favorito determinate categorie di persone, un algoritmo di quella tipologia addestrato su quei dati tenderà a fare lo stesso. La soluzione sta nella trasparenza e nella continua revisione dei modelli: bisogna sottoporli a test regolari e intervenire per correggere eventuali distorsioni. Inoltre, è fondamentale che chi sviluppa questi sistemi sia consapevole dei rischi e adotti pratiche di progettazione etica. Qui scendiamo un po' sul tecnico, ma penso che valga la



pena sottolineare che la frontiera sia di non far più apprendere dai token, ovvero dei dati esistenti: alcuni sistemi si basano già sul *chain of thoughts e sul reinforcement learning*. Alcuni ritengono che questo scenario possa rivoluzionare quanto finora conosciamo oggi, aprendo alcune frontiere attualmente non completamente esplorate.

Un altro aspetto fondamentale è la sicurezza informatica: quali sono i principali pericoli legati all'AI e come possiamo mitigarli?

L'AI, come qualsiasi altra tecnologia, è vulnerabile agli attacchi. Uno degli scenari più pericolosi è l'avvelenamento dei dati di addestramento: un hacker potrebbe inserire informazioni false in un sistema per influenzarne le decisioni. Pensiamo a un'AI che gestisce i prezzi di un mercato online: alterando i dati, si potrebbero manipolare le dinamiche di vendita. Per prevenire questi rischi, la sicurezza deve essere integrata fin dalla fase di sviluppo, con protocolli rigorosi e un monitoraggio costante. La parola chiave è proattività: non è più possibile aspettare che un problema si manifesti per intervenire.

Di fronte a queste sfide, è quindi possibile garantire un utilizzo sicuro ed etico dell'intelligenza artificiale o servono ulteriori interventi?

Le aziende devono dotarsi di regolamenti chiari che definiscano gli standard minimi di sicurezza, la trasparenza nei processi decisionali e la protezione dei dati, assumendosi la responsabilità di sviluppare tecnologie etiche. Non va trascurato l'aspetto comunicativo nei confronti dei collaboratori per spiegare loro al meglio le opportunità e i rischi di questi sistemi. Come sempre è la cultura aziendale a fare la differenza: l'AI deve essere introdotta in azienda secondo un approccio responsabile, che va definito fin dall'inizio. L'uso di tecnologie private nelle aziende, come ad esempio abbonamenti personali per migliorare la produttività, non inseriti in contesti chiari e condivisi, va assolutamente evitato.

A questo proposito, si parla sempre più spesso di "algoretica". Può spiegare meglio cosa significa e quale ruolo può avere in questo contesto?

L'algoretica è l'etica applicata agli algoritmi. In altre parole, si tratta di progettare sistemi di AI che rispettino principi morali condivisi. Un esempio classico è quello delle auto a guida autonoma: in caso di emergenza, come dovrebbero comportarsi? Proteggere il conducente a tutti i costi o cercare di minimizzare i danni complessivi? Sono dilemmi complessi, che richiedono un confronto tra esperti di tecnologia, etica e diritto. L'obiettivo è creare AI che non siano solo efficienti, ma anche giuste e responsabili, oltre a seguire le norme dello Stato in cui vengono applicate e non solo quelle dello Stato in cui vengono progettate e addestrate.

Guardando al futuro, quale messaggio principale ritiene più importante trasmettere su questo tema?

L'AI non è solo una questione tecnologica, ma anche sociale ed etica. La sicurezza non riguarda solo la protezione dei dati, ma anche la cultura, la trasparenza nei processi decisionali e l'equilibrio tra automazione e controllo umano. Serve un approccio flessibile, che permetta all'innovazione di crescere guadagnandosi la fiducia delle persone. L'intelligenza artificiale è una straordinaria opportunità, ma dobbiamo gestirla con responsabilità, per costruire un futuro in cui la tecnologia sia al servizio dell'umanità e non viceversa.

www.grupposicurezza.ch

