FONDAZIONE BRUNO KESSLER
MAGAZINE

Oltre la black box: la nuova governance della sicurezza

12 Luglio 2026

L’IA non è una moda passeggera, ma un fattore strutturale che trasforma i processi lavorativi e genera nuovi profili di rischio. Per questo motivo, la sua gestione non può restare confinata nei dipartimenti IT, né limitarsi a un semplice addendum burocratico al Documento di Valutazione dei Rischi. È necessaria una governance integrata che superi i "silos" tra sicurezza, privacy e diritti fondamentali.

Prosegue “**L’AI ci aiuta a lavorare meglio?”,** il confronto con Federico Cabitza, direttore del Centro di ricerca FBK-Digital Health and Wellbeing, analizziamo quali nuove competenze siano necessarie per chi oggi si occupa di protezione e prevenzione nei luoghi di lavoro.

Progettare l’integrazione dell’IA nel mondo del lavoro significa, prima di tutto, garantire che il suo impiego sia compatibile con la dignità, l’autonomia professionale e la responsabilità dei lavoratori.

Non è una sfida puramente tecnica: la vera innovazione risiede nel superamento dei “silos” burocratici, unendo la sicurezza sul lavoro (DVR), la privacy (DPIA) e la tutela dei diritti fondamentali (FRIA) in un’unica strategia integrata.

L’IA è un fattore strutturale che ridefinisce ruoli e competenze, e come tale richiede che il Servizio di Prevenzione e Protezione (SPP) diventi un attore strategico capace di interpretare non solo i dati, ma l’intero contesto socio-tecnico.

In questo secondo appuntamento, approfondiamo quali competenze siano necessarie per tradurre l’opacità degli algoritmi in fattori di rischio valutabili.

GS: Lei propone che il Servizio di Prevenzione e Protezione (SPP) diventi un attore strategico della governance dell’IA, uscendo dai “silos” tecnici per dialogare con IT, HR e uffici legali. Quali sono le competenze non-tecniche prioritarie che un/a addetto/a alla sicurezza dovrebbe acquisire oggi per riuscire a tradurre l’opacità di una “black box” algoritmica in fattori di rischio comprensibili e valutabili all’interno del Documento di Valutazione dei Rischi (DVR)?

FC: “Credo che il punto di partenza sia riconoscere che la black box non è solo un problema tecnico. È anche un problema organizzativo, cognitivo e decisionale. Naturalmente servono competenze tecniche, o almeno un’alfabetizzazione minima sui sistemi di IA: bisogna sapere che cos’è un modello predittivo, che cos’è un sistema generativo, che cosa significa errore, incertezza, bias, deriva del modello, validazione. Ma per il Servizio di Prevenzione e Protezione questo non basta.

La prima competenza non-tecnica è la capacità di analisi socio-tecnica del lavoro. Un sistema di IA non va valutato come oggetto isolato, ma come parte di un processo: chi lo usa, in quale momento, con quale grado di autonomia, sotto quale pressione temporale, con quali possibilità di contestazione, con quali effetti sulle responsabilità, sulle competenze e sulle relazioni di lavoro. Spesso il rischio non sta nel modello in sé, ma nel modo in cui il modello viene inserito nel processo organizzativo.

La seconda competenza riguarda l’analisi dei fattori umani. Un addetto alla sicurezza deve saper riconoscere fenomeni come automation bias, over-reliance, deskilling, perdita di situation awareness, affaticamento cognitivo, stress da monitoraggio continuo, dipendenza da raccomandazioni automatiche. Sono rischi meno visibili di quelli fisici, ma non per questo meno rilevanti. Se un lavoratore si abitua a non decidere più, o a non poter contestare un output algoritmico, siamo già dentro una trasformazione del rischio professionale.

La terza competenza è la capacità di traduzione interdisciplinare. Lo SPP non deve diventare un reparto di data science, ma deve essere in grado di fare le domande giuste a chi sviluppa, acquista o integra sistemi di IA. Domande del tipo: su quali dati è stato addestrato il sistema? In quali condizioni è stato validato? Che tipo di errore produce? Chi controlla gli aggiornamenti? Come viene gestito il dissenso dell’operatore? Cosa succede se il sistema sbaglia? Esistono log, audit trail, soglie di intervento, procedure di escalation?

La quarta competenza è giuridico-organizzativa. Non nel senso che lo SPP debba sostituirsi al legale, ma nel senso che deve comprendere il nesso tra rischio tecnologico, responsabilità, documentazione, tracciabilità e governance. Nel DVR non possiamo limitarci a scrivere che “è stato introdotto un sistema di IA”. Dobbiamo descrivere come quel sistema modifica l’attività lavorativa, quali rischi introduce o amplifica, quali misure tecniche, organizzative e formative sono state previste, e chi è responsabile del controllo nel tempo.

Infine, serve una competenza metodologica: la capacità di valutare evidenze. Una tecnologia non è sicura perché il fornitore la presenta come innovativa, né perché funziona in una demo. Va valutata nel contesto reale d’uso. Questa è una delle idee centrali della proposta di valore del DHWB: aiutare imprese, istituzioni e in generale decisori e policy maker a comprendere se, come e a quali condizioni una tecnologia digitale o un sistema di IA possa generare valore sanitario, cioè clinico, organizzativo e sociale, in modo sicuro, sostenibile e responsabile.”

Segnali di allarme silenziosi

Una governance moderna deve saper mitigare rischi nuovi come la *Techno-complexity* o lo stress da opacità decisionale. Governare l’IA significa anche saper leggere i cambiamenti invisibili nel benessere dei lavoratori. Prossimamente, nel capitolo conclusivo di questa serie, vedremo come identificare i “segnali sentinella” di un possibile disagio psicologico legato all’interazione con le macchine “intelligenti”.

LINK

https://magazine.fbk.eu/it/news/oltre-la-black-box-la-nuova-governance-della-sicurezza/

TAG

- #prevenzione
- #salutedigitalebenessere
- #sicurezza

AUTORI

- Giancarlo Sciascia