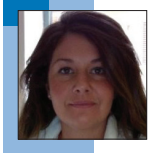
Stefania Calosso
Avvocato civilista,
componente della Rete Giuridica AIAS



Chiara Piccaglia De Eccher
Avvocato penalista,
componente della Rete Giuridica AIAS

Sicurezza sul lavoro o sicurezza del lavoro?

Il paradosso della sicurezza nell'era digitale tra nuove vulnerabilità e vecchie responsabilità

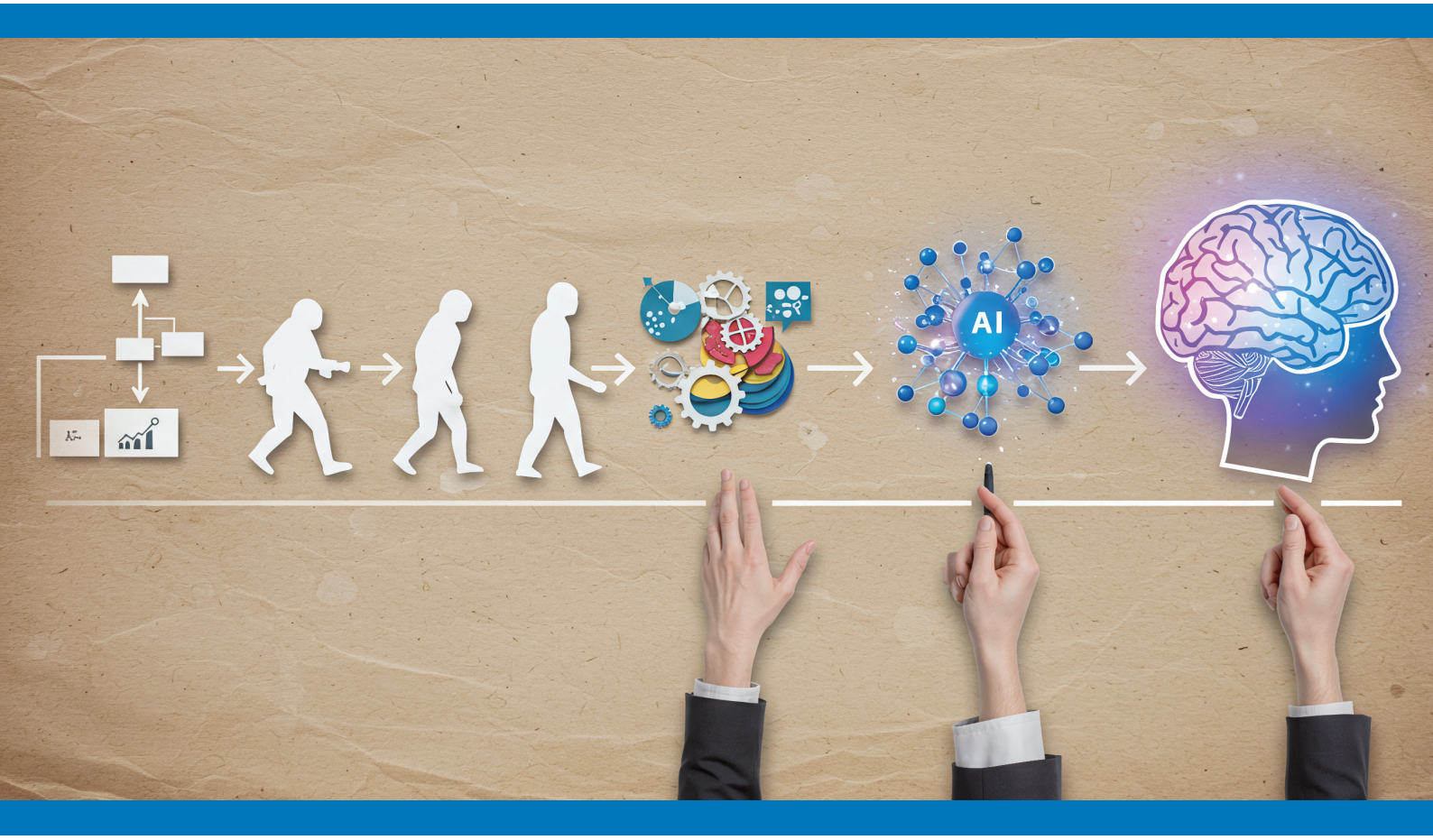
Nell'era digitale, la distinzione tra sicurezza sul lavoro e del lavoro si dissolve. Gli ambienti lavorativi sono ecosistemi ibridi dove fisico e digitale si intrecciano, generando vulnerabilità inedite. Attacchi cyber possono causare danni fisici, mentre la manipolazione di dati personali impatta sulla salute psicofisica. Emerge un nuovo paradigma di rischi integrati che sfuggono alle categorie tradizionali.

La domanda che apre questa riflessione non è meramente retorica: la distinzione, apparentemente sottile, tra sicurezza *sul* lavoro e sicurezza *del* lavoro nasconde una trasformazione epocale che sta ridefinendo i confini della tutela lavorativa.
Nell'era della trasformazione digitale, i luoghi di lavoro sono diventati ecosistemi ibridi dove il fisico e il digitale si intrecciano in maniera indissolubile.

Il panorama lavorativo contemporaneo è, infatti, pervaso da una capillare infrastruttura tecnologica (sensori *IoT* che monitorano la qualità dell'aria, sistemi di automazione industriale connessi in rete, dispositivi *wearable*s che tracciano i parametri vitali dei lavoratori, piattaforme collaborative *cloud-based* ecc.) che, se da un lato garantisce maggiore efficienza e controllo, dall'altro genera vulnerabilità inedite e rischi sistemici di portata senza precedenti che rendono obsoleto il tradizionale paradigma della sicurezza.
Quest'ultimo, invero, essendo edificato sui pilastri della prevenzione dei rischi fisici, chimici e biologici, si rivela strutturalmente inadeguato di fronte alla complessità dei moderni ambienti lavorativi digitalizzati.

Ma vi è di più. La compartimentazione tra sicurezza fisica e sicurezza logica, un tempo funzionale e operativamente giustificata, è diventata una fonte di vulnerabilità sistemica.

Consideriamo un caso emblematico
Un attacco *ransomware* che colpisce i sistemi di controllo di un impianto industriale può paralizzare i sistemi di sicurezza antincendio, compromettere i protocolli di evacuazione automatizzati, o disattivare i sistemi di monitoraggio ambientale.



In questo scenario, la distinzione tra *cybersecurity* e *safety* diventa non soltanto accademica, ma controproducente: il danno fisico origina da una vulnerabilità digitale, e la responsabilità del datore di lavoro si estende inevitabilmente dal dominio fisico a quello *cyber*.

Sotto altro profilo, va rilevato che le nuove frontiere del rischio hanno dato origine a vulnerabilità emergenti la cui tassonomia è costituita da una gamma di rischi che sfuggono alle categorie tradizionali della sicurezza lavorativa, che qui elenchiamo.

Rischi psicosociali amplificati

I sistemi di monitoraggio digitale dei lavoratori, se compromessi o mal configurati, possono generare forme di sorveglianza invasiva che producono stress cronico, ansia da controllo e deterioramento del benessere psicofisico; inoltre, la manipolazione illecita di questi dati può creare dinamiche discriminatorie o ricattatorie che impattano direttamente sulla salute mentale dei lavoratori.

Rischi da interruzione di servizio

La crescente dipendenza da sistemi digitali per il funzionamento di infrastrutture critiche rende i lavoratori vulnerabili alle conseguenze di malfunzionamenti o attacchi informatici; l'interruzione dei sistemi di climatizzazione, illuminazione, comunicazione interna o gestione degli accessi può creare situazioni di pericolo immediato per la salute e l'incolumità fisica.

Rischi da manipolazione dei dati

L'alterazione illecita di dati relativi alla sicurezza – dai parametri ambientali ai protocolli di emergenza, dalle certificazioni di sicurezza ai registri di manutenzione – può compromettere l'efficacia dei sistemi di prevenzione e creare falsi sensi di sicurezza con conseguenze potenzialmente catastrofiche

Rischi di manipolazione dei dati personali

Si pensi (*i*) alla manipolazione dei dati biometrici e di quelli relativi alla salute effettuata dai sistemi di monitoraggio della salute sul lavoro (un attacco che alteri i dati del monitoraggio cardiaco di un lavoratore addetto a mansioni ad alto rischio potrebbe impedire l'identificazione tempestiva di situazioni di emergenza medica); (*ii*) alla alterazione dei profili di competenza e formazione (l'alterazione fraudolenta di un database formativo potrebbe far risultare un lavoratore come "formato" su procedure di sicurezza che in realtà non conosce, esponendolo ed esponendo i colleghi a rischi gravissimi).

Rischi di manipolazione dei sistemi di geolocalizzazione

I sistemi di tracciamento GPS utilizzati per monitorare la posizione dei lavoratori in ambienti pericolosi o isolati, se manipolati possono nascondere situazioni di pericolo, ritardare i soccorsi, o creare false comunicazioni di emergenza.

Rischi di alterazione dei dati di accesso e autorizzazione

I sistemi di controllo degli accessi basati su dati personali (impronte digitali, riconoscimento facciale, *badge* personalizzati) possono essere compromessi per consentire l'accesso non autorizzato ad aree pericolose o per impedire l'accesso a lavoratori autorizzati in situazioni di emergenza.

Gli **impatti psicosociali** della manipolazione dei dati personali sono enormi: la consapevolezza o il sospetto che i propri dati personali possano essere stati manipolati genera effetti psicologici devastanti sui lavoratori quali perdita di fiducia nei sistemi di sicurezza, ansia da controllo, stress cronico, deterioramento delle relazioni interpersonali; ancora, tali effetti, oltre a compromettere il benessere individuale, possono ridurre la capacità di attenzione e di reazione del lavoratore, aumentando indirettamente il rischio di infortuni.