**Stefania Calosso**
Avvocato, Cultrice della materia Data Protection Law presso l'Università di Bologna, componente della Rete Giuridica AIAS

**Chiara Piccaglia De Eccher**
Avvocato penalista, Socio AIAS

# Sicurezza sul lavoro o sicurezza del lavoro?

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

**L'art. 2087 CC richiede un'interpretazione evolutiva che consideri le vulnerabilità cyber. La governance della sicurezza deve superare le compartimentazioni tra RSPP e CISO. Tre pilastri guidano la transizione: integrazione normativa, formazione strategica e tecnologia alleata. La sfida è trasformare la complessità in azione concreta per garantire ambienti lavorativi resilienti nell'era digitale.**

**La prima parte del contributo è pubblicata nel numero 39 di aiasmag**
**www.aias-sicurezza.it/aiasmag**

Dal punto di vista del datore di lavoro, la manipolazione dei dati personali pone quest'ultimo di fronte a un duplice ordine di responsabilità. Da un lato, la responsabilità ex art. 32 GDPR per la mancata protezione dei dati personali; dall'altro, la responsabilità per i danni alla salute e sicurezza dei lavoratori derivanti dall'uso di dati compromessi per decisioni operative. Questa convergenza di responsabilità richiede un approccio integrato alla protezione dei dati che consideri non solo gli aspetti *privacy* e di protezione dei dati personali, ma altresì le implicazioni *safety* delle violazioni.
Il D.Lgs. 81/2008, pur nella sua lungimiranza, non poteva anticipare la pervasività dell'odierna digitalizzazione del lavoro. Tuttavia, i principi fondamentali che lo ispirano – la tutela dell'integrità fisica e della personalità morale del lavoratore, l'obbligo di valutazione e prevenzione di tutti i rischi per la salute e la sicurezza – mantengono piena validità e richiedono oggi un'interpretazione evolutiva che tenga conto delle nuove dimensioni del rischio.
L'art. 2087 del Codice Civile, norma di chiusura del sistema di tutela lavoristica, impone al datore di lavoro di adottare

> *le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.*

In un contesto digitalizzato, questa formulazione assume una portata rivoluzionaria: "l'esperienza e la tecnica" contemporanee impongono necessariamente la considerazione delle vulnerabilità cyber come par-

te integrante dell'ecosistema di rischi da presidiare.
La complessità del nuovo panorama di rischi richiede, pertanto, un approccio alla *governance* della sicurezza che superi le tradizionali compartimentazioni organizzative. Il Responsabile del Servizio di Prevenzione e Protezione (RSPP) non può più prescindere da competenze di *cybersecurity*, così come il *Chief Information Security Officer* (CISO) non può ignorare le implicazioni *safety* delle vulnerabilità informatiche.

**In conclusione**la responsabilità per la sicurezza integrata *sul* lavoro e *del* lavoro deve essere chiaramente allocata a livello organizzativo adottando un approccio sistemico alle vulnerabilità integrate. Quest'ultimo deve fondarsi su tre pilastri: l'**integrazione normativa**, la **formazione strategica** e la **tecnologia alleata**. Segnatamente:

### Integrazione normativa

L'attuale frammentazione normativa tra disciplina della sicurezza sul lavoro e regolamentazione della *cybersecurity* rappresenta un ostacolo alla realizzazione di un approccio integrato alla sicurezza, tanto che si rende necessario un intervento legislativo che riconosca esplicitamente l'interconnessione tra sicurezza fisica e logica, (ri)definendo chiaramente le responsabilità del datore di lavoro nell'era digitale.

### Formazione strategica

La transizione verso un modello di sicurezza integrata richiede un massiccio investimento in formazione a tutti i livelli organizzativi, dai lavoratori operativi, che devono sviluppare con-

sapevolezza delle implicazioni di sicurezza delle loro azioni digitali, sino agli apicali, che devono comprendere le implicazioni strategiche e legali delle nuove vulnerabilità per potervi far fronte.

### Tecnologia alleata

Paradossalmente, la stessa tecnologia se da un lato genera nuove vulnerabilità, può, dall'altro lato, fornire strumenti innovativi per la loro gestione.

Ad esempio, l'intelligenza artificiale applicata alla sicurezza può consentire il monitoraggio in tempo reale delle minacce *cyber* con potenziale impatto sulla *safety*, mentre i sistemi di *machine learning* possono identificare *pattern* anomali che precedono gli incidenti.


### Conclusivamente

si ritiene che la domanda, volutamente provocatoria, con la quale si è aperto questo contributo, trova nella complessità dell'ecosistema lavorativo contemporaneo una risposta che supera la dicotomia iniziale: non si tratta più di scegliere tra sicurezza *sul* lavoro e sicurezza *del* lavoro, ma di riconoscere che nell'era digitale questi due paradigmi convergono in un'unica, inscindibile dimensione della tutela lavorativa.

Le "vecchie responsabilità" del datore di lavoro in materia di prevenzione e protezione non sono quindi obsolete, ma richiedono un'interpretazione evolutiva che tenga conto delle nuove vulnerabilità generate dalla digitalizzazione.

L'obbligo di sicurezza si estende oggi dal dominio fisico a quello *cyber*, dalla protezione dei corpi alla tutela dei dati, dalla prevenzione degli infortuni alla prevenzione degli attacchi informatici con ricadute sulla *safety*. Questa evoluzione richiede un cambio di paradigma culturale prima ancora che normativo: la sicurezza deve essere ripensata come un ecosistema integrato dove competenze tecniche, organizzative e umane convergono nella costruzione di ambienti lavorativi resilienti e sicuri.

Il futuro della sicurezza del lavoro sarà necessariamente digitale, ma dovrà rimanere profondamente umano nei suoi obiettivi fondamentali: la tutela dell'integrità, della dignità e del benessere di chi lavora. In questo senso, le nuove vulnerabilità dell'era digitale non fanno che riaffermare l'attualità e l'urgenza delle "vecchie responsabilità" che da sempre caratterizzano il rapporto di lavoro: proteggere chi lavora, in tutte le sue dimensioni e contro tutti i rischi, vecchi e nuovi che siano.

La sfida che ci attende è, pertanto, quella di trasformare la consapevolezza di questa nuova complessità in azione concreta: normativa, organizzativa, formativa. Solo così potremo garantire che la rivoluzione digitale del lavoro sia anche una rivoluzione della sua sicurezza.