

■ A. Staffieri analizza il fenomeno della cyberviolenza

OLTRE LO SCHERMO: PERCHÉ LA CYBERVIOLENZA È IL NUOVO RISCHIO INVISIBILE DEL TUO UFFICIO (E COSA DICE LA LEGGE)*

DI LUCA DI SEVO CONSULENTE DEL LAVORO IN BOLLATE (MI)

L'evoluzione delle tecnologie dell'informazione e della comunicazione (ICT) ha ridefinito i confini della prestazione lavorativa, ma ha anche aperto il fianco a un rischio sociale emergente: la *cyberviolenza*. Oggi, la distinzione tra spazio digitale privato e professionale può essere messa seriamente in discussione. Un'azione apparentemente esterna, consumata su un *social network*, può scuotere seriamente le fondamenta di un'intera organizzazione, minando il benessere dei dipendenti e la solidità dei processi interni. È nuovamente tempo di riconoscere che la sicurezza non finisce dove inizia la rete. In questo contesto si è ravvisato che la cosiddetta violenza digitale non è una minaccia eterea, ma una realtà con ripercussioni materiali che possono rivelarsi molto serie. I dati testimoniano una preoccupante normalizzazione della cultura misogina che impatta direttamente sulla carriera e sulla vita delle lavoratrici:

- Oltre un terzo delle donne a livello globale ha subito violenza digitale.

- Il 75% delle vittime censite teme per la propria incolumità fisica.
- Il 7% delle vittime arriva a perdere il lavoro o è costretto a dimettersi, dimostrando che il danno "virtuale" si traduce rapidamente in un danno economico e professionale concreto.

"Il 35% delle vittime ha riportato danni alla salute mentale, un dato che equipara gli effet-

ti delle aggressioni digitali a quelli della violenza fisica in termini di stabilità psicologica." Quando una risorsa abbandona il proprio ruolo a causa di abusi *online*, l'azienda affronta un fallimento non solo operativo ma soprattutto etico.

Si aggiunge a questo il cosiddetto "*Digital Wellness Deficit*" attorno a cui si configura il nuovo volto dello *stress*, cagionato dall'adozione massiccia di modelli come lo *smart working* e il telelavoro. Uno squilibrio, causato dall'iperconnessione costante, agisce da facilitatore per abusi invisibili ma profondamente lesivi. Si è ravvisato che l'anonimato percepito e l'assenza di un confronto fisico immediato possono favorire un'*escalation* di comportamenti vessatori. Per l'azienda, questo può tradursi in costi occulti enormi: aumento dell'assenteismo, calo del rendimento e un *turnover* elevato. Da un punto di vista personale, la violenza digitale mina l'autostima della vittima e contribuisce a rendere tossico il clima aziendale, trasformando lo *stress* lavorativo in una condizione cronica.

IL GLOSSARIO DEL RISCHIO

Per gestire il rischio, è necessario padroneggiare la terminologia tecnica e le dinamiche psicologiche sottostanti:

- *Doxing*: diffusione illecita di dati sensibili (indirizzi, numeri privati, dati bancari) tramite *phishing*, *IP tracking* o strumenti di *Whois* ➤

* Sintesi dell'articolo pubblicato in D&PL, 46/2025, pag. 2681 dal titolo *Cyberviolenza: rischio emergente per le organizzazioni e tutele*.

per intimidire la vittima e distruggerne la reputazione professionale.

- *Sextortion*: estorsione basata sulla minaccia di diffondere materiale sessualmente compromettente. Fa leva strategicamente sul senso di colpa e di vergogna della vittima per paralizzare ogni tentativo di denuncia.
- *Revenge Porn* (Pornovendetta): diffusione non consensuale di contenuti espliciti per umiliare la lavoratrice. Le conseguenze includono isolamento sociale e, nei casi più gravi, tendenze autolesive.
- *Cyberstalking*: persecuzione reiterata via ICT (messaggi minacciosi, monitoraggio costante) che genera uno stato di ansia cronica e altera radicalmente le abitudini di vita.

Queste pratiche sfruttano la vulnerabilità psicologica per isolare la persona (più frequentemente di sesso femminile) dal proprio contesto di supporto, inclusi i colleghi e i superiori.

LA RESPONSABILITÀ AZIENDALE NELL'ARTICOLO 2087 C.C.

Le piattaforme digitali utilizzate per la prestazione lavorativa sono, a ogni effetto di legge, spazi professionali. In questo scenario, il datore di lavoro agisce come titolare dell'obbligo di garanzia.

Ai sensi dell'articolo 2087 del Codice Civile, l'azienda ha il dovere giuridico di adottare tutte le misure necessarie a tutelare l'integrità psicofisica dei dipendenti.

Ciò suggerisce un'azione precisa: il rischio di cyberviolenza deve essere integrato nel Documento di Valutazione dei Rischi (DVR). Non è più ammissibile considerare la sicurezza digitale come una questione di "autodifesa delle vittime". L'assenza di protocolli preventivi e formativi espone l'organizzazione a pesanti responsabilità risarcitorie e a un danno reputazionale incalcolabile.

TUTELE PER LE VITTIME DI CYBERVIOLENZA

L'ordinamento italiano e la contrattazione collettiva più avanzata offrono strumenti concreti per i cosiddetti "percorsi di fuoriuscita":

- Congedo per vittime di violenza (D.lgs. 15 giugno 2015, n. 80): è un diritto soggettivo (non discrezionale per il datore) che permette un'astensione dal lavoro fino a 90 giorni, indennizzata al 100%. Il CCNL Metalmeccanica rappresenta un'eccellenza, estendendo il congedo fino a 6 mesi: i primi 3 mesi sono a carico dell'Inps, mentre i successivi 3 sono interamente retribuiti dall'azienda.
- Assegno di Inclusione (AdI): con la Legge di Bilancio 2025 questa misura è stata potenziata. Le donne vittime di violenza in carico ai Centri Antiviolenza sono considerate in "condizione di svantaggio", garantendo loro un sostegno economico strutturale per favorire l'autonomia.
- Reddito di Libertà: si tratta di un contributo fino a 400 euro mensili per 12 mesi, reso strutturale dalla Legge di Bilancio 2024, destinato all'autonomia abitativa e personale.
- Flessibilità e mobilità: il CCNL Metalmeccanica riconosce il diritto al trasferimento in altre sedi, la trasformazione del contratto in *part-time* (senza subordinazione alla disponibilità di organico) e forme di flessibilità oraria o *smart working* per mettere in sicurezza la lavoratrice.

VERSO UN'ETICA DELLA DIGNITÀ DIGITALE

La cyberviolenza non è un problema di "software", ma di cultura organizzativa. Le aziende leader oggi non si limitano a reagire alle emergenze, ma promuovono un'etica della disconnessione e del rispetto attraverso codici di condotta stringenti e formazione specifica. La sicurezza sul lavoro nel XXI secolo passa necessariamente per la bonifica degli spazi digitali.