PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4192 di Giovedì 08 marzo 2018

Nuovi rischi per i lavoratori: le ICT

Le tecnologie dell'informazione e della comunicazione modificando i riferimenti contestuali e gli ambienti di lavoro, espongono i lavoratori anche a nuove forme e fattori di rischio quali violazione della privacy, violazioni di norme e cyberbullying.

Lo sviluppo delle tecnologie dell'informazione e della comunicazione (ICT) in ambito lavorativo può avere un impatto sulla salute e la sicurezza dei lavoratori, a causa dell'eccessivo carico di lavoro, del sovraccarico informativo e della mancanza di separazione tra vita privata e vita professionale esponendo la persona a continue interruzioni e intromissioni. È frequente, infatti, che si verifichino sistematiche comunicazioni private nei luoghi di lavoro in cui vengono rese pubbliche le proprie soddisfazioni emotive o familiari, conducendo la per sona verso una costante transizione psicologica dalla modalità office alla modalità home e viceversa, con compromissione della qualità e della diversificazione dei livelli di comunicazione e di interazione. Tutto ciò potrebbe diminuire il contatto personale nelle relazioni, aumentando l'isolamento sociale e peggiorando le relazioni esistenti. Le ICT modificando i riferimenti contestuali e gli ambienti di lavoro, espongono i lavoratori anche a nuove forme e fattori di rischio quali violazione della privacy, violazioni di norme e cyberbullying.

DESCRIZIONE

Privacy e violazioni di norme

Emerge la necessità di gestire e regolare in maniera adeguata, anche attraverso l'istituzione di apposite policy, il processo di innovazione tecnologica che interessa tutte le organizzazioni. A livello normativo la direttiva 95/46/CE è stata emanata con l'obiettivo di proteggere le persone in materia di trattamento dei dati personali, affermando il diritto alla privacy e la necessità di individuare le figure responsabili del trattamento per la protezione dei dati. I datori di lavoro (DL), in riferimento all'uso di social networking (SN), nell'ambito delle policy aziendali dovrebbero tenere conto non solo del rispetto dei requisiti di legge richiesti, ma anche di eventuali responsabilità penali a causa di uno scorretto uso di SN da parte dei propri dipendenti. Le comunicazioni su queste piattaforme, infatti, potrebbero invadere la privacy di una persona, essere diffamatorie e, se denigratorie, causare stress emotivo o anche istigare comportamenti illeciti. In generale dunque, sotto la teoria di respondeat superior, i DL sono indirettamente responsabili per gli illeciti che i dipendenti commettono nel corso del rapporto di lavoro. Con il d.lgs. 151/2015, inoltre, è stata introdotta la possibilità di controllare a distanza - previo accordo con le parti interessate, le rappresentanze sindacali o gli enti di competenza attraverso impianti audiovisivi e altri strumenti tecnologici - il lavoratore e l'attività lavorativa, limitatamente ad alcune ipotesi così come riportato in Tabella 1

Tabella 1	Controllo con dispostivi elettronici sul lavoro
Consentito	**Non consentito**
Esigenze organizzative e produttive.	Finalità unica ed esclusiva del controllo a distanza del lavoratore.
Sicurezza del lavoro.	Controllo massivo, prolungato e indiscriminato dell'attività del lavoratore.
Tutela del patrimonio aziendale.	Accesso in maniera indiscriminata a posta elettronica o ai dati personali contenuti negli smartphone in dotazione al personale.

Il DL, pur avendo la facoltà di verificare l'esatto adempimento della prestazione professionale ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, deve in ogni caso salvaguardarne la libertà e la dignità, attenendosi ai limiti previsti dalla normativa. I lavoratori, inoltre, devono essere sempre informati in modo chiaro e dettagliato sulle modalità di utilizzo degli strumenti aziendali e delle eventuali verifiche a distanza.

Violenza sul lavoro e molestie

La violenza e le molestie sul lavoro, secondo i dati europei del 2011, interessano una percentuale di lavoratori compresa tra il 5% e il 20% e sebbene il 40% dei dirigenti si dichiari preoccupato in merito a tali fenomeni, solo il 25% - e in alcuni Paesi non più del 10% - ha posto in atto procedure, politiche o strategie per fronteggiarli. Negli ultimi anni, secondo Eurofound, emerge la presenza di diverse forme di violenza fisica e/o psicologica che interagiscono e si sovrappongono al punto da renderne difficile una netta distinzione. In generale si assiste alla diminuzione del fenomeno della violenza fisica, e ad un aumento di nuove forme di violenza quali minacce, intimidazioni, bullismo, molestie e attenzione sessuale indesiderata. Secondo l'Agenzia europea per la sicurezza e la salute sul lavoro, un lavoratore su sei in Europa ha subito violenze e molestie anche a sfondo sessuale e sono in aumento i casi legati al bullismo, in Italia conosciuto con il termine mobbing, che influisce negativamente sulla salute e sul benessere dei lavoratori (2014). In questo contesto all'inizio del 2016, anche in Italia, le parti sociali e datoriali hanno siglato un'intesa che recepisce l'Accordo Quadro sulle molestie e la violenza nei luoghi di lavoro, sottoscritto il 26 aprile del 2007 dalle rispettive rappresentanze a livello europeo.

AMBITI DI APPLICAZIONE E IMPATTI SULLA SSL

Già nel 2010 all'interno delle linee guida europee multisettoriali contro la violenza e le molestie sul lavoro, il cyberbullying veniva definito come un rischio emergente a causa della crescente pervasività e uso delle ICT e dei dispositivi mobili nei luoghi di lavoro. Il fenomeno si caratterizza, come nel caso del bullismo, attraverso i criteri della ripetizione di atti vessatori, comportamenti ostili e negativi verso la vittima e disparità di livello tra la vittima e l'autore della molestia. In Tabella 2 sono

riportate le principali caratteristiche relative alle molestie e bullismo online.

Malgrado siano ancora pochi gli studi relativi all'analisi di tale fenomeno nei luoghi di lavoro, alcune indagini hanno evidenziato quanto i nuovi mezzi di comunicazione digitale possano modificare i riferimenti contestuali e gli ambienti di lavoro stessi; tendenzialmente quando sono online le persone hanno minore consapevolezza dei rischi e sono meno prudenti nella valutazione delle situazioni di pericolo rispetto all'ambiente fisico. Le caratteristiche dei mezzi di comunicazione digitali tenderebbero secondo altri studi a promuovere conflitti e incomprensioni riferiti a legami deboli e ai concetti espressi.

L'esposizione a comportamenti e atti di cyberbullying, infine, secondo recenti studi è correlata ad un aumento di tensione mentale, insoddisfazione lavorativa, isolamento e stanchezza mentale.

CONCLUSIONI

Diversamente dalle forme di bullismo tradizionale la modalità online tende ad essere, anche a causa della pervasività del mezzo utilizzato, molto più evidente e visibile e può quindi avere maggiori conseguenze anche sulla reputazione aziendale. Le persone spesso utilizzando gli strumenti tecnologici in maniera inconsapevole non si rendono conto delle potenzialità negative dell'esposizione pubblica delle informazioni pubblicate e della loro permanenza sulla rete. Per questo motivo è auspicabile la definizione di social media policy in relazione ai materiali e contenuti che vengono postati in rete non solo in merito alle attività lavorative ma anche in relazione ai commenti relativi a colleghi. Le aziende dovrebbero sviluppare e sostenere politiche reali contro le molestie e il bullismo anche attraverso un'adeguata formazione che accompagni l'osservanza di queste policy contribuendo alla diffusione di una cultura di prevenzione.

Tabella 2	Caratteristiche molestie e b
Cyberharrassment Molestia online che differisce dalla tipologia di molestia tradizionale proprio a causa della natura tecnologica e digitale del mezzo attraverso - il molestatore (uomo o donna) può essere anonimo o meglio non esplicitare la propria identità; - la vittima (uomo o donna) può essere assente nel momento in cui viene commesso l'atto di molestia; - le intimidazioni sono estese al di fuori dell'orario lavorativo poiché la tecnologia consente il perpetuare dell'atto 24 h al giorno per 365 gio - l'abuso può essere replicato velocemente e quasi all'infinito (foto, pubblicazione di dati sensibili e password della vittima); - più persone possono partecipare e condividere la molestia come nel caso dei social media ad esempio; - gli effetti sul lavoratore possono essere diversi rispetto al fenomeno tradizionale.	
Cyberbullying Forma di prevaricazione volontaria e ripetuta nel tempo, attuata mediante uno strumento digitale ai danni di un singolo individuo o gruppo co e mettere a disagio la vittima di tale comportamento, che non riesce a difendersi. Smith (2006) definisce il fenomeno attraverso sette categorie centrate sugli strumenti utilizzati: - sms invio e ricezione di messaggi testuali offensivi e diffamatori attraverso il telefono cellulare; - mms invio e ricezione di materiale multimediale (foto/video) recante danno a terze persone; - calls invio e ricezione di chiamate diffamatorie, in cui l'aggressore intimidisce la vittima con minacce e insulti; - e-mail invio di mail contenenti insulti, minacce, offese e diffamazioni; - chatrooms intimidazioni e offese in chat; - instant message insulti e offese tramite sistemi di comunicazione istantanea (come MSN, Yahoo, Skype, WhatApp, Messenger, ecc.); - websites rivelazione di informazioni personali o divulgazione di immagini e video compromettenti (per la vittima) attraverso siti internet. Willard (2006) propone invece una tassonomia alternativa del fenomeno centrata sul tipo di azione e di comportamento perpetrato: - flaming messaggi violenti e volgari che mirano a suscitare contrasti e battaglie verbali nei forum; - harassment (molestie) invio ripetuto di messaggi offensivi e sgradevoli; - denigration (denigrazione) insultare o diffamare qualcuno online attraverso dicerie, pettegolezzi e menzogne, solitamente di tipo offensi danneggiare la reputazione di una persona e i suoi rapporti; - impersonation (furto d'identità) l'aggressore ottiene informazioni personali e dati di accesso (nick, password, ecc.) di un account della vitt prenderne possesso e danneggiarne la reputazione; - outing and trickering diffondere online i segreti di qualcuno, informazioni scomode o immagini personali; spingere una persona, attraverso informazioni imbarazzanti e riservate per renderle poi pubbliche in rete; - exclusion (esclusione) escludere intenzionalmente qualcuno/a da un gruppo online (chat, liste di amici, forum tematici, ecc.); - doxing diffusione pubblica via internet di dati personali e sensibili; - cyberstalking invio ripetuto di messaggi intimidatori contenenti minacce e offese.	

INAIL - ICT: DISTORSIONI D'USO (PDF)

www.puntosicuro.it