

LE NUOVE TECNOLOGIE: USI E RISCHI

Attacchi esterni, data breach, atti persecutori e mobbing orizzontale sono i principali rischi di un uso improprio delle nuove tecnologie in ambito aziendale.

Il tema del **diritto alla privacy** è sempre più di attualità, soprattutto al giorno d'oggi, quando lo si vede costantemente lesa proprio dagli strumenti che dovrebbero consentire il progresso e, di conseguenza, il miglioramento delle condizioni di vita.

Per poter analizzare tale aspetto anche in funzione delle tematiche lavorative, occorre innanzitutto chiarire quelli che sono i diritti fondamentali dei lavoratori, che non vanno mai lesi: *Ogni lavoratore ha diritto a **condizioni di lavoro sane, sicure e dignitose*** (Carta di Nizza, art. 31); *dignità e libertà* sono due concetti chiave, ribaditi nel titolo I dello Statuto dei Lavoratori (Legge 300

del 1970); *La dignità umana è inviolabile e deve esser rispettata e tutelata*, concetto espresso nella Carta dei diritti fondamentali dell'Unione Europea (la cosiddetta "Carta di Nizza"), all'art. 1.

Qualora tali strumenti raccogliessero informazioni personali del dipendente, in caso di *data breach* l'azienda si ritroverebbe a fronteggiare un serio pericolo, anche per l'incolumità dei propri dipendenti.

A fronte di tali premesse, occorre porre l'attenzione su un tema che, se non considerato con il giusto peso, rischia di avere dei risvolti anche penali a danno dell'imprenditore inadempiente o, semplicemente, poco avveduto. Posto che l'art. 4 dello Statuto dei Lavoratori impone il divieto di installazione di impianti audiovisivi o di apparecchiature di controllo a distanza senza un previo accordo con RSA e senza aver prima informato il personale dipendente e che tale divieto può essere derogato solo in presenza di esigenze organizzative, produttive, di tutela del patrimonio aziendale e previo accordo con RSA e DTL, possiamo ora ad analizzare i rischi latenti che possono emergere da un eventuale utilizzo improprio degli strumenti elettronici.

In primo luogo, se **hackerati** questi apparecchi rischiano di trasformarsi da utili strumenti di controllo del dipendente e di tutela del patrimonio aziendale in accessi facilitati per quegli stessi elementi esterni da cui l'azienda intendeva difendersi.

Altro pericolo latente per l'azienda è quello di ledere uno dei diritti fondamentali del lavoratore, ossia quello alla **riservatezza**. Qualora, infatti, tali strumenti raccogliessero informazioni personali del dipendente, in caso di *data breach* (vedasi, ad esempio, dati biometrici, stato di salute o abitudini dell'utente ad esso riconducibili), l'azienda si ritroverebbe a fronteggiare un serio pericolo, anche per l'incolumità dei propri dipendenti.

Quando, ancora, si installasse un sistema di **geolocalizzazione** sui dispositivi portatili in grado di collegare il dispositivo all'utilizzatore, troverebbe applicazione la normativa sulla privacy (D. Lgs. 196/2003) che vedrebbe lesi i diritti dell'utente, con le relative conseguenze del caso.

Visti i tempi critici che stiamo attraversando, sono sempre più diffusi gli abusi perpetrati proprio con l'utilizzo di strumenti tecnologici, come gli attacchi esterni ad aziende di varia importanza. Altro tema, questo, su cui occorre riflettere per poter difendere e tutelare il patrimonio aziendale.

Sempre in considerazione dei tempi difficili, non mancano, tuttavia, episodi di **atti persecutori** attuati da aziende in crisi in danno ai dipendenti. Può capitare, infatti, che alcuni imprenditori disonesti utilizzino strumenti tecnologici e persone secondo modalità non consentite dalla legge. Alcune aziende con budget in discesa libera assumono figure quali i **"tagliatori di teste"**, l'esatto opposto dei "cacciatori di teste", che studiano la psicologia dei soggetti "sacrificabili" e, ledendo e attaccando i punti deboli dei malcapitati, portano avanti il piano di "snellimento" con tutte le tecnologie e le tecniche a loro disposizione.

Il rischio peggiore a cui l'azienda può andare incontro, così come accaduto in passato a molti amministratori delegati, è che le vittime arrivino, loro malgrado, a togliersi la vita (reato penale configurabile con l'**istigazione al suicidio**).

Capita, inoltre, che tali atti persecutori vengano attuati da pari grado, a totale insaputa del datore di lavoro, ravvisando l'ipotesi di **mobbing orizzontale**. Anche in quest'ultimo caso, il datore di lavoro che non abbia vigilato e non possa dimostrare che tali comportamenti dipendano da cause a lui non imputabili si troverebbe a dover fronteggiare problematiche di rilevanza penale.

Qualora l'imprenditore, per controllare i dipendenti, utilizzasse strumenti quali virus/worm/spam su dispositivi ad essi in uso, si vedrebbe passibile di **condanna penale**.

Il trattamento illecito dei dati può comportare, infatti, **responsabilità penali, sanzioni amministrative e responsabilità civile** ed è punibile se arreca nocumento all'interessato e al suo patrimonio.

Occorre, quindi, meditare a lungo su quanto la tecnologia possa essere un utile alleato e quanto, invece, possa diventare un tremendo nemico. Non mandiamo dunque in pensione le vecchie abitudini, non del tutto desuete.

Alcune aziende con budget in discesa libera assumono figure quali i "tagliatori di teste", che studiano la psicologia dei soggetti "sacrificabili" e portano avanti il piano di "snellimento".

VALERIA ROSA

