

PRIVACY E DATA BREACH: COME DIFENDERSI E TUTELARSI

Da utile alleato, la tecnologia usata in modo improprio o fraudolento può mettere a rischio i nostri dati e quelli dei nostri clienti.

Il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo tutelato dal Codice in materia di protezione dei dati personali (D.Lgs 196/2003).

Il diritto alla privacy è riconosciuto dall'art. 7 del Codice Privacy e dal diritto all'oscuramento dei dati nei casi previsti dalla legge. Visti i tempi a dir poco difficili che stiamo attraversando e i mille volti che ai giorni nostri assume la criminalità, occorre, soprattutto nella nostra professione, porre l'attenzione sulla materia sotto molteplici profili e sfaccettature.

Nel nostro caso specifico, ove i dati trattati, oltre ai nostri stessi, sono quelli dei nostri clienti, occorre mantenere alta l'attenzione sul tema e fornire istruzioni alla clientela.

I nostri dati, come richiesto dal Ministero della Giustizia, sono inseriti negli albi e accessibili a chiunque, pertanto sono facilmente reperibili anche da impostori e truffatori. Sempre più diffuso ai nostri giorni è il reato di **furto di identità** (o *data breach*) ma, quando ci si accorge di esserne vittime, i danni patiti sono ormai irrecuperabili o quasi. Qualora vengano violati i dati per accesso abusivo ai nostri sistemi di comunicazione, il fornitore di servizi deve, senza ritardo, comunicare la violazione al Garante, ai sensi dell'art. 32 bis del D.Lgs 196/2003.

In caso di *data breach*, stante la complessità e il numero dei sistemi in essere presso i fornitori, **occorre fornire alle Autorità competenti informazioni dettagliate relative alle violazioni verificatesi, purché ciò avvenga subito dopo l'avvenuta conoscenza della stessa.**

Tali informazioni devono consentire alle Autorità di valutare l'entità della violazione e devono comprendere:

- i dati identificativi del fornitore;
- una descrizione della violazione subita;
- l'indicazione della data della presunta violazione e del momento della sua scoperta;
- l'indicazione del luogo in cui è avvenuta la violazione dei dati, specificando se sia avvenuta a seguito di smarrimento di dispositivi.



Sempre più spesso, inoltre, capita di esser vittime di **accessi abusivi ai nostri sistemi informatici** da cui occorre difendersi e tutelarsi per proteggere i nostri dati e quelli dei nostri clienti.

Altro tema importante nella nostra professione riguarda i **controlli a distanza negli ambienti di lavoro**. Va specificato che per controlli a distanza si intendono quelli effettuati tramite l'utilizzo di apparecchiature e "sistemi tecnologici".

L'art. 4 dello Statuto dei Lavoratori, poi modificato dal D.Lgs 151/2015 per effetto della legge delega n. 183/2014 (in arte Job Act), ha consentito l'installazione di impianti audiovisivi e di strumenti di controllo se funzionali allo svolgimento dell'attività lavorativa, previo accordo sindacale autorizzato dalla DTL.

Non è necessario accordo, invece, per gli strumenti (ad es. smartphone, tablet, ecc) che servano al dipendente per svolgere attività lavorativa, purché sia fornita allo stesso l'informativa come previsto dal codice privacy. Diventano, poi, utilizzabili a fini disciplinari le informazioni assunte tramite tali strumenti di controllo.

Le fonti normative di riferimento sono l'art. 4, 28 e 38 Legge 300/1970 e l'art. 171 del D.Lgs 196/2003.

CONTROLLI A DISTANZA

Con tale espressione si fa riferimento a quelli che in gergo si indicano come "controlli tecnologici". Occorre però considerare la linea sottile che separa il controllo a distanza con la lesione dei diritti fondamentali del lavoratore sanciti, tra l'altro, anche nella nostra Costituzione.

I Garanti Europei sanciscono infatti che «se è vero che le nuove tecnologie costituiscono un'evoluzione, così per quanto riguarda le risorse a disposizione dei datori di lavoro gli strumenti di vigilanza elettronica si prestano ad essere utilizzati in modo tale da ledere i diritti e le libertà fondamentali dei dipendenti». **La dignità umana va anteposta a qualsiasi altra considerazione.**

Così come sancito dalla nostra Costituzione «la libertà personale è inviolabile», così come lo è la segretezza della corrispondenza e di ogni altra forma di comunicazione, altrettanto lo è il rispetto della vita privata dell'individuo.

L'ambiente di lavoro, così come ribadito dall'art. 2 della Carta costituzionale, deve assicurare l'esplicazione della personalità umana. Questo poco si confà al controllo e alla sorveglianza delle comunicazioni, quali lesioni della libertà dell'individuo.

Il divieto posto all'art. 4 dello Statuto dei lavoratori è assoluto ma può esser superato in presenza di esigenze organizzative, produttive e di sicurezza o tutela del patrimonio aziendale.

Il divieto di effettuare controlli a distanza riguarda altresì il dipendente che, autonomamente, decida di effettuare riprese per finalità investigative private, che lo vedrebbero passibile di sanzioni disciplinari a proprio carico.

Va da sé che tale controllo può esser effettuato soltanto su dispositivi di proprietà dell'azienda stessa e non del singolo dipendente. In tal caso, qualora il controllo fosse effettuato su mezzi di comunicazione propri del dipendente, si configurerebbe un reato penale a carico dell'autore, normato altresì dal D.Lgs 231/2001.

I **controlli tecnologici** all'interno delle strutture aziendali potrebbero diventare, però, **strumento utile alle Autorità nelle controversie in casi di "mobbing" o "straining"**.

Per concludere, possiamo affermare che la tecnologia, se usata con moderazione, può diventare un utile alleato, ma qualora se ne faccia un uso improprio, smodato o addirittura fraudolento, può diventare assai pericolosa.

Utile sarebbe riflettere e confrontarsi sull'argomento.

Buon lavoro.

VALERIA ROSA

È sottile la linea che separa il controllo a distanza con la lesione dei diritti fondamentali del lavoratore, essendo «la libertà personale inviolabile» (art. 2 della Costituzione).