26 febrero 2020

Smart working e protezione dei dati: disposizioni del Governo per contrastare l'emergenza Coronavirus

Milano, 26 febbraio 2020 – Lo **smart working** é stato introdotto nel nostro ordinamento dalla **Legge 81 del 2017**.

L'art. 18 della L. 81/2017 lo definisce quale "*modalità flessibile di esecuzione del rapporto di lavoro subordinato allo scopo di incrementarne la produttività e agevolare la conciliazione dei tempi di vita e di lavoro.*"

Con lo smart working il lavoratore può operare da remoto con l'utilizzo di strumenti tecnologici per svolgere la propria prestazione, percependo la stessa retribuzione dei colleghi che svolgono la stessa mansione all'interno dell'azienda.

Di regola, per l'avvio dello smart working occorre, secondo la Legge 81/2017, un accordo individuale lavoratore-aziende, che

- specifichi nel dettaglio tempi e modi di utilizzo degli strumenti che permettono di lavorare da remoto, e cioè pc portatili, tablet e smartphone;
- garantisca parità di trattamento economico e normativo rispetto ai colleghi che eseguono la prestazione con modalità ordinarie;
- predisponga forme di tutela in caso di infortuni e malattie professionali.

Quest'accordo va poi registrato sul portale del Ministero del Lavoro.

Con il **DPCM del 23 febbraio 2020 il Governo**, "ritenuta la straordinaria necessità ed urgenza di emanare disposizioni **per contrastare l'emergenza epidemiologica da Covid-19**, adottando misure di contrasto e contenimento alla diffusione del predetto virus" **è intervenuto per rendere più immediato il ricorso allo smart working nelle aree considerate a rischio** per l'emergenza **Coronavirus**.

Peraltro un nuovo **DMCM**, messo a punto nella giornata di ieri, **25 febbraio**, contiene un importante chiarimento in merito all'**ambito di applicazione della disciplina semplificata**, specificandone la validità non solo nella cosiddetta **zona rossa** (i 10 comuni lombardi e l'unico veneto individuati come focolaio del contagio) ma anche in tutte le Regioni a rischio, cosiddetta **zona gialla**, che vengono elencate espressamente (Emilia Romagna, Friuli Venezia Giulia, Lombardia, Piemonte, Veneto e Liguria).

In tali aree, dunque, per favorire il normale svolgimento dell'attività lavorativa è consentita, in via straordinaria, l'attivazione dello smart working anche in assenza dell'accordo individuale, tramite una procedura telematica dove l'accordo individuale è sostituito da un'autocertificazione che il lavoro agile si riferisce ad un soggetto appartenente a una delle aree a rischio; quanto all'informativa sulla sicurezza del lavoro, essa può essere assolta anche tramite una semplice email, utilizzando la documentazione resa disponibile sul sito dell'Inail. Questa modalità semplificata sarà utilizzabile in via transitoria e per un periodo molto breve (sino al 15 marzo 2020, salvo eventuali futuri rinnovi della disciplina).

La situazione di emergenza rappresenta una grande **sfida** alla resilienza delle **aziende** non solo sotto il profilo della loro capacità di cogliere le opportunità dell'evoluzione del lavoro ma anche sotto quello dell'adeguatezza rispetto al tema della **sicurezza dei dati**.

Attraverso i propri dispositivi, infatti, lo smart worker entra continuamente in contatto con i database aziendali e tratta una mole non indifferente di informazioni, a volte sensibili. L'accesso, inoltre, non avviene all'interno delle mura aziendali, ma dalla sua abitazione o – peggio – da altri luoghi esterni, amplificando le probabilità che i dati possano essere visualizzati o prelevati da altri (si pensi, a mero titolo di esempio, alle criticità sollevate dalle rete wi-fi libere che si trovano in molti locali che idealmente si prestano a fungere da luoghi di coworking).

L'azienda, in qualità di titolare o responsabile del trattamento, è tenuta a **garantire la sicurezza costante dei dati** e a mettere in atto le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato a norma degli **articoli 24 e 32 del GDPR**, la cui violazione può esporla a **sanzioni pecuniarie fino a 10 milioni di euro o fino al 2% del fatturato totale annuo mondiale**.

In che modo?

Innanzitutto partendo dalla **protezione dei dispositivi** attraverso l'installazione di adeguati software antivirus ed efficienti sistemi di backup e la messa a punto di strategie di Mobile Device Management (MDM) che prendano in considerazione tecnologie di password authentication, data encryption, remote wipe/lock (per formattare da remoto i dispositivi e cancellare tutti i dati in caso di furto o smarrimento).

Inoltre dotandosi di adeguate **policy e procedure**, che non solo vengano portate a conoscenza degli utenti ma con essi condivise attraverso una mirata attività di formazione, che potrà essere svolta anche con l'aiuto del DPO aziendale, se presente, affrontando, nello specifico, proprio quei temi che possono presentare particolari aderenze con lo smartworking, come ad esempio i numerosi comportamenti quotidiani che possono portare a potenziali rischi quali lo smarrimento dei device o la navigazione tramite reti non sicure.

Una buona formazione in azienda risulterà tanto più fondamentale oggi in considerazione del fatto che, stando agli esperti, in concomitanza con l'attuale crisi sanitaria l'Italia risulta nel mirino dei cybercriminali, intenzionati ad approfittarsi del minore stato di allerta degli utenti lanciando campagne volte a infettare i computer delle aziende per sottrarre dati o estorcere danaro. Ciascuna campagna comprende più attacchi destinati a più soggetti, comprendendo un numero elevato di aziende e bersagli all'interno di queste.

Spesso gli attacchi sfruttano tecniche di ingegneria sociale per convincere le vittime ad aprire gli allegati o i link, magari sul Coronavirus, i quali sono spesso documenti contenenti macro che scaricano e installano i malware.

La migliore tecnica per scongiurare questi attacchi è quella di non aprire mai e in nessun caso allegati da fonti che non siano note e conosciute e comunicare la ricezione al personale IT aziendale. Anche email all'apparenza molto ben fatte e scritte in italiano perfetto possono celare minacce alla sicurezza aziendale. Bisogna dunque sempre valutare attentamente cosa si va ad aprire controllando l'oggetto, il mittente, l'indirizzo email di provenienza e così via. Sono controlli semplici che portano via poco tempo, ma che possono già aiutare a scremare le email dannose; in ogni caso è bene sospettare sempre e chiedere sempre aiuto al personale competente.

_____

DISCLAIMER

Il presente comunicato è divulgato a scopo conoscitivo per promuovere il valore dell’informazione giuridica. Non costituisce un parere e non può essere utilizzato come sostitutivo di una consulenza, né per sopperire all’assenza di assistenza legale specifica.