Smart working e rischi informatici

whynery.com/smart-working-e-rischi-informatici

10 dicembre 2020

Dietro le Quinte

David Scaffaro – 10 Dicembre 2020

Nella presente rubrica verranno trattati temi relativi agli obblighi legislativi, alle certificazioni volontarie ed a temi, considerati "no core" per le aziende, che possono avere un impatto determinante per le sorti delle stesse.

Verranno analizzati, con un linguaggio comprensibile a tutti, aspetti che normalmente sfuggono alla quotidianità delle attività svolte in azienda e, per quanto sia possibile, verrà seguito un filo logico sui distinti temi.

Gli aspetti legislativi, normativi e regolamentari rappresentano, oggi più che mai, un rischio spesso trascurato proprio perché poco percepito in quanto relativo ad attività ritenute improduttive.

Quindi, se sugli aspetti legislativi si approfondiranno le singole tematiche richiamate, i potenziali rischi e le azioni da condurre per il loro abbattimento con la conseguente protezione dell'azienda, per le certificazioni volontarie si analizzeranno le opportunità, i miglioramenti e lo sviluppo che questi possono apportare.

Si tratteranno aspetti diversi tra loro, dalla sicurezza informatica alla salute e sicurezza sul lavoro, fino ai temi ambientali e di privacy.

Tutti temi che si legano indissolubilmente alle attività dell'imprenditore moderno.

Lo smart working

Lo smart working è una modalità di lavoro che introduce una **maggiore flessibilità nell'attività svolta dal lavoratore**. Tale flessibilità, fa si che il lavoratore possa impostare i propri processi lavorativi gestendo gli ambienti dove svolgere le attività, la strumentazione necessaria o che reputa maggiormente perfomante, gli orari e i carichi di lavoro.

Sostanzialmente può trovare ed attuare **le migliori strategie per raggiungere determinati obiettivi**.

Telelavoro e smart working

Il termine smart working viene usato, solitamente, in un'eccezione molto ampia e spesso in **modo improprio.**

In realtà il telelavoro e lo smart working hanno **caratteristiche lavorative piuttosto differenti**, sia concettualmente, sia da un punto di vista giuridico.

Il telelavoro, a differenza dello smart working, prevede una postazione fissa di lavoro, pur se a distanza rispetto la sede convenzionale, un orario rigido e in linea con quello effettuato nella sede aziendale, limitata o nulla libertà nelle decisioni strategiche di gestione delle attività lavorative e la possibilità del datore di lavoro di controllare gli orari di lavoro.

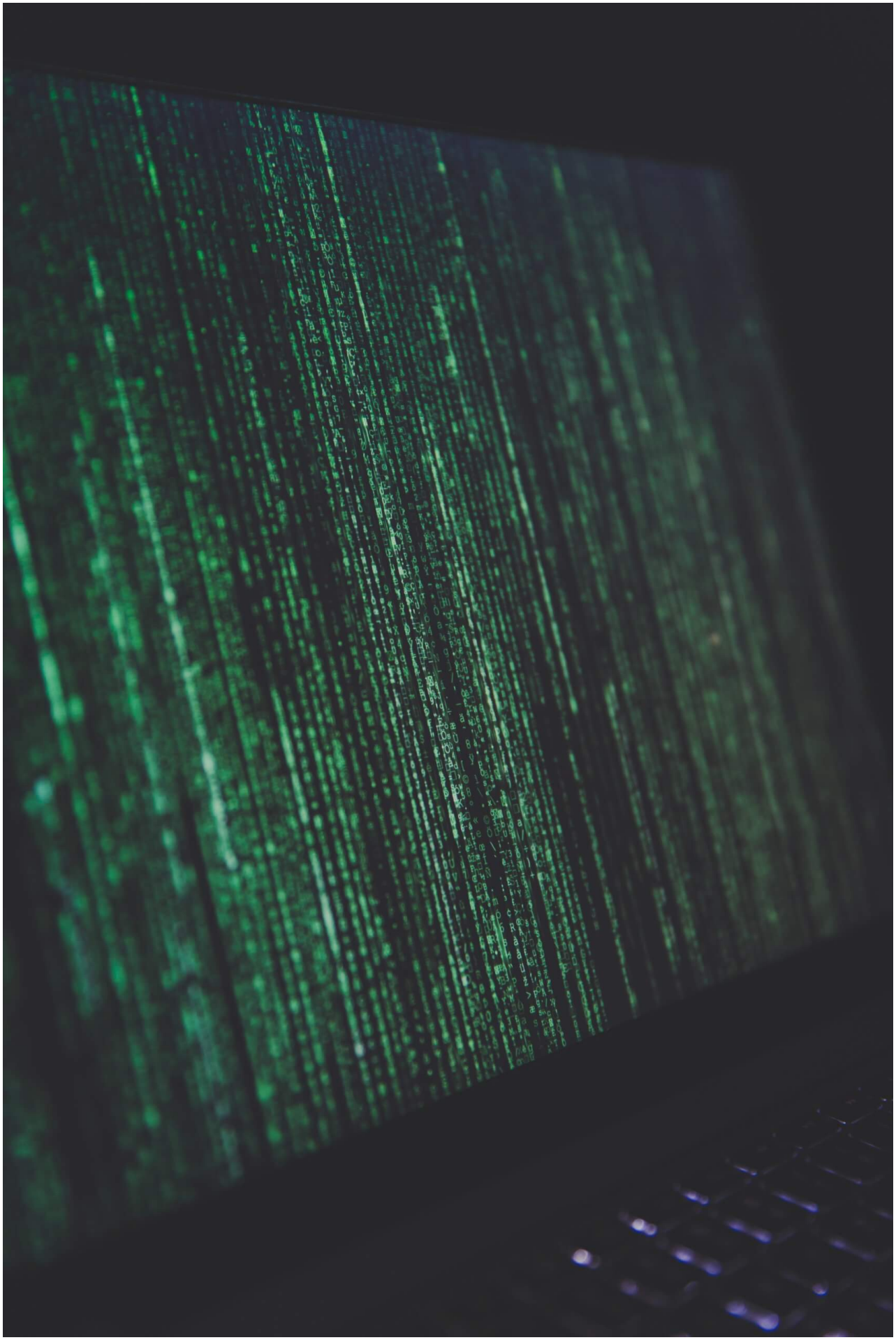
Quindi **il telelavoro è una sorta di fedele trasposizione presso il domicilio**, o altro luogo preposto, del lavoro svolto normalmente presso la sede aziendale

Smart Working e normativa applicabile

Lo smart working è regolato, in principio, **dalla Legge 81 del 22 Maggio 2017**.

La suddetta legge ha sancito per la prima volta alcuni aspetti interessanti, come la possibilita che questo sia a tempo determinato o indeterminato, oppure la pari copertura infortunistica rispetto al lavoratore non in smart working.

Inoltre, a seguito della pandemia da Sars-CoV-2, sono state emanate normative di tipo emergenziale che hanno di fatto, incoraggiato ed accelerato la modalità di lavoro in smart working.



Dispositivi di proprietà del lavoratore

La proprietà degli strumenti da utilizzare, con particolare riferimento a quelli informatici, **può essere del datore di lavoro oppure del lavoratore.**

Questo può dipendere dalle clausole contrattuali in essere; generalmente in condizioni di **telelavoro la dotazione hardware e software è di proprietà dell'azienda**, mentre nello **smart working i devices e i software utilizzati sono normalmente di proprietà del lavoratore.**

Rischi relativi alla sicurezza informatica

Solitamente **i dispositivi aziendali hanno un grado di sicurezza maggiore dei dispositivi personali**.

Ciò dovuto anche alle **policy aziendali sulla cybersecurity**.

L'utilizzo di **dispositivi personali, quindi, alza generalmente il grado di rischio relativo alla sicurezza delle informazioni**.

Le cause di maggiori rischi in tal senso possono ricondursi, ad esempio, ai seguenti aspetti:

- mancato utilizzo di adeguati software antimalware
- obsolescenza degli aggiornamenti delle firme virali dei software antimalware
- errato settaggio dei software antimalware
- software VPN inaffidabili
- utilizzo promiscuo del device, ovvero interazione tra uso lavorativo e uso privato
- utilizzo di password deboli
- impostazioni di sicurezza dei browser assenti
- mancanza di interazione tra specifici e diversi software di sicurezza
- inadeguata formazione sulla sicurezza informatica
- campagne di phishing e smishing
- utilizzo di reti non sicure

Impatto sui reati informatici

Lo sviluppo delle nuove tecnologie è stato lo stimolo all'intervento legislativo che nel 1993, tramite **la Legge 547/93, ha introdotto nel codice penale il reato di "frode informatica" (Art. 640-ter)**, estendendo ed ampliando il reato di truffa (Art. 640), già previsto dal codice penale.

Un successivo passo si è dato con l'emanazione della **Legge 48/08**, ovvero la ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita' informatica, redatta a Budapest il 23 novembre 2001. **Questa, oltre ad apportare modifiche ad alcuni articoli del codice penale, ha introdotto l'art. 24-bis. (Delitti informatici e trattamento illecito di dati) nel D.Lgs. 231/01.**

L'art. 24-bis del D.Lgs. 231/01 prevede la sanzionabilità dei seguenti articoli: 615-ter,

617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies, 615-quater, 615-quinquies, 491-bis e 640-quinquies, con una fornice sanzionatoria amministrativa da **100 a 500 quote** (615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies), **fino a 300 quote** (615-quater, 615-quinquies), **fino a 400 quote** (491-bis e 640-quinquies). Il valore di ogni quota oscilla da un **minimo di 258 euro ad un massimo di 1549 euro**.

Nel GDPR

Per quanto riguarda **il GDPR**, nella sezione 2, relativa alla sicurezza dei dati dati personali, **l'art. 32 richiede una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento**. Inoltre, nel caso di **data breach** e nella seguente notifica di violazione dei dati personali all'autorità di controllo **(art. 33)**, **l'azienda dovrà descrivere le misure adottate**, o di cui si propone l'adozione, da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. Le sanzioni amministrative massime sono fino a **20.000.000 di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore**. Va detto, comunque che spesso le sanzioni sono di importo minore, poichè si applica il concetto che queste devono essere effettive, proporzionate e dissuasive.

Considerazioni

La tendenza al lavoro a distanza e allo smart working, oltre ai benefici e vantaggi per aziende e lavoratori, **mostra anche il suo lato negativo, legato ai rischi relativi alla sicurezza informatica e alla commissione di reati informatici, previsti dal codice penale e facenti parte integrante del D.Lgs. 231/01 e richiamati nel GDPR.**

Le aziende **possono mitigare i propri rischi redigendo dei robusti sistemi documentali in ambito legislativo (D.Lgs. 231/01 e GDPR), attuando performanti architetture dei sistemi di sicurezza informatica e fornendo un'adeguata formazione ai propri lavoratori.**

Scopri il nostro online store

Registrati, profila la tua identità sensoriale ed accedi allo store Whynery.

Vai al Login

Lascia un commento

Autenticato come David Scaffaro. Uscire?