

SMART WORKING

Maggio 2020
Ver. 1.0



AARON
TECHNOLOGY

IN QUESTO NUMERO

1. Che cos'è lo smart working?
2. Aspetti legali collegati allo smart working
 - a. Suggerimenti pratici e domande frequenti
 - b. Condotte del lavoratore
 - c. Domande frequenti
3. Sicurezza del lavoro e smart working
4. Strumenti tecnologici e sicurezza dei dati
5. Aspetto organizzativo interno all'azienda

"Il lavoro a distanza è il futuro del lavoro."
(Alexis Ohanian)

1. CHE COS'È LO SMART WORKING?

«Lo Smart Working (o Lavoro Agile) è una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli orari o spaziali e un'organizzazione per fasi, cicli e obiettivi, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività».

Ministero del Lavoro e delle Politiche Sociali

Si tratta di un nuovo modo di lavorare dove è possibile trovare un buon equilibrio tra la qualità della vita e la produttività di ciascuno e dove un corretto uso delle nuove tecnologie consente l'integrazione e la collaborazione all'interno dell'organizzazione, oltre che una modalità efficace di interazione con l'esterno.

Smart working non significa in modo riduttivo "lavorare da casa" con la disponibilità di qualche strumento tecnologico, significa invece un cambio totale di paradigma, dove sono coinvolti tutti i modelli organizzativi dell'azienda. L'ufficio diventa "aperto" e non è più legato ad un luogo fisico.

Gli ambiti coinvolti nel cambio di Modello sono molti, per cui non si può e non si deve improvvisare, si tratta di **un complesso cambiamento** essenzialmente **culturale**, ma anche **manageriale** che coinvolge l'intera organizzazione.

La **Digital Transformation** che stiamo attuando nelle nostre organizzazioni con l'applicazione di tecnologie innovative, assume qui un ruolo determinante e necessario, volto a realizzare il concetto chiave dei nostri tempi: "la connessione", affinché si sia tutti coinvolti e produttivi.

Per poter concretizzare un modello di Smart Working è necessario attingere a diverse discipline che possono aiutare a meglio identificare la portata del nuovo paradigma lavorativo. Riteniamo fondamentali i seguenti aspetti:

- Legale (Normativa)
- Sicurezza del Lavoro
- Tecnologie, connessione e sicurezza dei dati
- Organizzazione interna dell'azienda (strumenti e disponibilità dei dati)
- Modello di leadership



AARON
TECHNOLOGY

2. SMART WORKING – ASPETTI LEGALI

Il lavoro agile è disciplinato dalla Legge 22 maggio 2017 n. 81 – Misure di tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato. Gli articoli dedicati al tema sono i seguenti:

Nello specifico:

ART. 18: il lavoro agile costituisce **una nuova modalità di organizzazione del lavoro**, in cui l'attività lavorativa viene svolta in parte all'interno dei locali aziendali e in parte all'esterno, senza una postazione fissa, ma nel rispetto dei limiti di durata massima dell'orario di lavoro giornaliero e settimanale stabiliti dalla legge e dai CCNL.

ARTT. 19-20: l'accordo relativo alle modalità di lavoro agile è stipulato per iscritto;

l'accordo individua i tempi di riposo e le misure tecniche ed organizzative per la disconnessione del lavoratore; il lavoratore in lavoro agile ha diritto al medesimo trattamento retributivo dei lavoratori che svolgono la medesima attività lavorativa nei locali aziendali.

ART. 21: l'accordo individuale regola l'esercizio dei poteri di controllo e disciplinare da parte del datore di lavoro.

ART. 22: il datore di lavoro consegna, ogni anno, al lavoratore e al rappresentante dei lavoratori per la sicurezza una **informativa scritta** contenente i rischi generali e specifici connessi alla particolare modalità di svolgimento del rapporto di lavoro. Il lavoratore è tenuto a cooperare all'attuazione delle misure di prevenzione predisposte dal datore di lavoro riguardo la prestazione eseguita all'esterno dei locali aziendali.

ART. 23: il lavoratore agile ha diritto **alla tutela contro gli infortuni** anche quando occorsi in itinere e all'esterno dei locali aziendali.

Per i lavoratori che lavorano in smart working la legge prevede **un trattamento economico e normativo identico ai dipendenti** che svolgono il lavoro presso la sede dell'azienda. La parità è assicurata anche grazie alla **tutela INAIL** (circolare n. 48/2017) per gli infortuni e le malattie professionali.

E' disponibile una [piattaforma dedicata](#), disposta dal Ministero del Lavoro, dove è possibile **depositare gli accordi di smart working**. Per accedere occorre avere lo SPID. I dati da indicare sono i seguenti:

- i dati del datore di lavoro
- i dati del dipendente
- la tipologia di lavoro agile (tempo determinato o indeterminato)
- la durata del lavoro agile.

2.a SUGGERIMENTI PRATICI E DOMANDE FREQUENTI

Device tecnologici, computer, connessione ecc.

IL DATORE DI LAVORO HA L'OBBLIGO DI FORNIRLI? Il Datore di lavoro non ha l'obbligo di fornire i device tecnologici. La norma prevede che il datore di lavoro sia responsabile della sicurezza e del buon funzionamento degli strumenti tecnologici per lo svolgimento del lavoro.

CONNESSIONE A INTERNET: il dipendente deve usare una connessione ad Internet per effettuare lo smart working. La legge prevede che il rimborso dei costi sostenuti dal dipendente per l'uso della connessione alla rete,

costituisce "rimborso di spese di interesse esclusivo del datore di lavoro anticipate dal dipendente. Per le ragioni esposte, ai rimborsi in questione non vanno applicate da parte del sostituto le relative ritenute fiscali, previdenziali e assistenziali" (risoluzione 357/E del 2007 dell'Agenzia delle Entrate).

LAVORO STRAORDINARIO: è consentito effettuare **lavoro straordinario anche in smart working**, dietro esplicita autorizzazione del datore di lavoro o se questi lo richieda preventivamente. In ogni caso la prestazione si deve svolgere entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva.

TICKET RESTAURANT nel caso in cui in azienda si faccia uso della mensa, se il dipendente lavora da casa, il datore di lavoro **non è tenuto a dare alcun ticket restaurant**, anche in situazioni di emergenza.

2.b CONDOTTE DEL LAVORATORE

Testo tratto dal Memo SMART WORKING E POTERE DISCIPLINARE E DI CONTROLLO - QUALCHE PRECAUZIONE redatto dallo **Studio legale Tonucci & Partners e distribuito da Confapi**

- 1) Occorre redigere un accordo individuale con gli smart worker?
- 2) Occorre arricchire tale accordo con clausole specifiche atte a fare sì che le condotte siano corrette?

La risposta a entrambi i quesiti è positiva.

Ora, ciò che intendiamo esaminare è quali previsioni possono aiutare il datore nel contrastare efficacemente condotte colpose o intenzionali in grado di ledere l'interesse aziendale.

A. VIOLAZIONE DI SEGRETI INDUSTRIALI DA PARTE DELLO SMART WORKER

Il primo e più significativo tema su cui l'effettuazione della prestazione "da remoto" pone problemi è quello della violazione dei segreti industriali.

Di seguito, un esempio, di clausola che potrebbe risultare utile.

Clausola n. 1

«In aggiunta a quanto previsto nel CCNL applicato in azienda, l'inosservanza da parte del Lavoratore della policy in tema di divieto di condivisione di informazioni industriali contenute all'interno degli strumenti tecnologici messi a disposizione dall'azienda per l'esercizio del lavoro in modalità agile sarà sanzionato secondo quanto previsto dall'art. ___ CCNL».

B. ESECUZIONE DI ATTIVITÀ DI LAVORO PER CONTO PROPRIO O DI TERZI DA PARTE DELLO SMART WORKER

Il secondo ambito in cui è utile spendere qualche considerazione è quello dello svolgimento da parte del lavoratore di attività incompatibili con la fedeltà di cui all'art. 2105 c.c.

Come ovvio, si tratta di una previsione che è presente in diversi CCNL, ma il peculiare contesto dello smart working fa sì che possa essere utile andare a colpire alcune condotte che potrebbero essere, per così dire, serventi.

Di seguito, un esempio, di clausola che potrebbe risultare utile.

Clausola n. 2

«In aggiunta a quanto previsto nel CCNL applicato in azienda, l'installazione da parte del lavoratore di software e/o applicativi sul pc portatile aziendale senza la preventiva autorizzazione del responsabile sarà sanzionata secondo quanto previsto dall'art. ___ CCNL».

C. NEGLIGENZA DELLO SMART WORKER

Il terzo ambito su cui è necessario soffermarsi è quella dell'effettività della prestazione di lavoro.

Il rischio concreto è che modalità improvvisate di attuazione dello smart working possano dare luogo ad uno svolgimento negligente e/o parziale della prestazione di lavoro da parte degli smart worker. Nessuno dubita

che lo smart working ponga il problema del controllo in termini del tutto diversi rispetto alla modalità ordinaria di svolgimento della prestazione di lavoro. Di seguito, un esempio, di clausola che potrebbe risultare utile.

Clausola n. 3

«In aggiunta a quanto previsto nel CCNL applicato in azienda, il mancato collegamento da parte del lavoratore agile nelle fasce orarie concordate sarà equiparato ad assenza ingiustificata e conseguentemente sanzionato secondo quanto previsto dall'art. ___ CCNL e ___ CCNL»

2.c DOMANDE FREQUENTI

A) POSSO CONTROLLARE GLI ACCESSI AD INTERNET DELLO SMART WORKER?

La frequenza degli accessi ad Internet dice molto circa la produttività del lavoratore; è, dunque, evidente l'interesse del datore ad esercitare un controllo a tale riguardo. Nondimeno, il controllo datoriale degli accessi e delle tipologie di siti consultati può costituire una violazione dell'art. 4 St. lav., il cui testo, novellato nel 2015, è richiamato espressamente dalla Legge 22 maggio 2017 n. 81. Sebbene il PC sia a ogni effetto uno, se non il principale, strumento di lavoro (ciò avvantaggia il datore per effetto dell'art. 4 comma 2 St. lav.) non mancano sentenze di merito (v. Trib. Torino, 19 settembre 2018 n. 1664) e prese di posizione dell'Autorità Garante per la Protezione dei Dati Personali (v. provvedimento 13 luglio 2016 n. 303) che risultano severe verso i datori e che potrebbero valere a maggior ragione in relazione a una forma (quella del lavoro agile) che presuppone a favore del dipendente la gestione libera del tempo di lavoro. La soluzione che si fa preferire è, dunque, quella del raggiungimento di un accordo con le rappresentanze sindacali aziendali che possa stabilire forme e modi di impiego delle apparecchiature in grado di dare luogo a forme di controllo a distanza. Fondamentale è anche il tema dell'informativa a fini privacy (art. 4, comma 3, St. lav.).

B) LO SMART WORKING È SOLO PER IL PERSONALE CHE SVOLGE MANSIONI DI CONCETTO?

Lo smart working è uno strumento che si indirizza fondamentalmente a manager, quadri ed impiegati. Il lavoro operaio non è formalmente escluso, ma presuppone spesso la contiguità dell'addetto con la macchina e questo rende insopprimibile la presenza del lavoratore sul luogo di lavoro (cantiere, fabbrica). Ciò che può verificarsi è la possibilità di fare ricorso al "lavoro a domicilio" (v. L. 18 dicembre 1973 n. 877) che per lavorazioni che non richiedono un processo produttivo lungo e complesso potrebbe ritornare in auge, specie presso le PMI.

C) IL LAVORATORE IN SMART WORKING DEVE NECESSARIAMENTE IMPIEGARE BENI STRUMENTALI DI PROPRIETÀ DEL DATORE O PUÒ USARE BENI DI SUA PROPRIETÀ?

La Legge 22 maggio 2017 n. 81 nel parlare al comma 2 dell'art. 18 di strumenti "assegnati" al lavoratore sembra esprimere una preferenza verso un assetto in cui il datore fornisce i beni al dipendente per poi esserne responsabile in punto sicurezza e buon funzionamento. D'altra parte, l'efficienza dello strumentario tecnologico concorre alla protezione di quei beni (segreti industriali) che, come abbiamo visto, possono essere difesi con la leva disciplinare, ma che ben possono essere attaccati anche da terzi (si pensi banalmente ai rischi di hacking che potrebbero essere acuiti da una gestione lassista da parte dell'imprenditore). Risulta, quindi, indubbio che la policy cosiddetta BYOD (bring your own device) sia rischiosa. Ognuno vede però come l'indicazione normativa non sia risolutiva (la legge non vieta al lavoratore di fare uso del suo PC personale) e la prassi (specie quella emergenziale delle ultime settimane) è nel senso di uno smart working alimentato dall'ampio ricorso a beni strumentali di proprietà del lavoratore.

D) POSSO REVOCARE LO SMART WORKING?

Come noto, lo smart working può essere attivato sia per i dipendenti a tempo determinato che a tempo indeterminato. In quest'ultimo caso, il datore di lavoro può revocare la modalità di lavoro agile con un preavviso di almeno trenta giorni (novanta per i lavoratori disabili). In alternativa, il lavoro agile può essere revocato con effetto immediato in caso di giustificato motivo. Il Legislatore non chiarisce i contorni del giustificato motivo, ma si può ipotizzare che, in presenza di effetti negativi sull'andamento economico e/o organizzativo dell'azienda, l'efficacia dell'accordo possa essere revocata.

3. SICUREZZA DEL LAVORO

Testo fornito dalla società SQ+ del **Dott. Moreno Cervelli** specializzata in Sicurezza del lavoro

Quali sono gli obblighi del datore di lavoro e quelli del lavoratore per un lavoro agile in sicurezza e nel rispetto delle leggi:

Premessa

Il lavoratore che svolge la propria prestazione lavorativa in regime di "smart working", per i periodi nei quali si trova al di fuori dei locali aziendali, deve cooperare con diligenza all'attuazione delle misure di prevenzione predisposte dal datore di lavoro; allo stesso tempo il datore di lavoro deve continuare a garantire la salute e la sicurezza del lavoratore, con un'informazione e una formazione adeguate.

Il DL infatti consegna al lavoratore e al rappresentante dei lavoratori per la sicurezza, con cadenza almeno annuale, un'informazione scritta nella quale sono individuati i rischi generali e i rischi specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro e provvede anche ad una formazione iniziale e periodica degli smart workers.

Il DL dovrà anche sottoporre gli smart workers ad una sorveglianza sanitaria nei casi previsti (es. uso del VDT > 20h/settimana).

Il lavoratore, al contempo è tenuto a cooperare all'attuazione delle misure di prevenzione predisposte dal datore di lavoro per fronteggiare i rischi connessi all'esecuzione della prestazione all'esterno dei locali aziendali.

Luogo di lavoro

Per garantire una maggiore tutela in termini di sicurezza e salute sul lavoro, lo smart working andrebbe svolto in un luogo privato, evitando luoghi pubblici quali giardini, parchi, sale d'attesa, bar, ristoranti, palestre, ecc. ad ogni modo il luogo pubblico non è vietato purché si possa operare in un ambiente idoneo.

Lo smart worker non deve dimenticare che l'ambiente di lavoro, per quanto privato, deve comunque rispettare i requisiti di sicurezza e il lavoratore è tenuto a seguire le informazioni e le buone prassi ricevute in sede di formazione generale e specifica.

Un posto di lavoro che rispetti una corretta ergonomia è la migliore premessa per garantire il benessere lavorativo e di conseguenza, un buon rendimento sul lavoro. I fattori negativi o dannosi per la salute e sicurezza si possono eliminare adottando adeguate misure tecnico organizzative.

Arredi scorretti dal punto di vista ergonomico provocano tensioni muscolari continue accompagnate da crampi, una scarsa illuminazione può affaticare gli occhi, provocare sensazioni di spossatezza e cali di concentrazione. Per questo è importante pensare alla prevenzione degli infortuni o ad evitare situazioni di malessere al momento di pianificare gli spazi adibiti ad ufficio. La progettazione dell'ambiente e della postazione di lavoro, deve assicurare che la collocazione delle attrezzature (video, tastiera, stampante, ecc.) e la dimensione degli spazi e le caratteristiche degli arredi siano funzionali alle esigenze dell'attività da svolgere

Attrezzature

Viene in genere fornito un PC portatile. L'impiego prolungato dei computer portatili necessita della fornitura di una tastiera e di un mouse o altro dispositivo di puntamento esterni nonché di un idoneo supporto che consenta il corretto posizionamento dello schermo.

È importante regolare in modo ottimale l'inclinazione dello schermo e anche la sua luminosità e il contrasto.

Illuminazione

Un ambiente di lavoro deve essere dotato di sufficiente illuminazione naturale, eventualmente integrata da sistemi di illuminazione artificiale anche localizzati.

La corretta illuminazione di un luogo di lavoro deve essere tale da garantire una buona visibilità per svolgere correttamente la propria attività; Inoltre, al fine di evitare l'affaticamento visivo, deve essere garantito un livello di illuminazione compatibile con l'impegno visivo richiesto dall'attività lavorativa. A tal fine, per l'illuminazione artificiale, il parametro di riferimento utilizzato è l'illuminamento definito come il rapporto tra il flusso luminoso che incide su di una superficie e l'area della superficie stessa e si misura in Lux. I valori di illuminamento raccomandati sono compresi tra 300 - 750 Lux. Devono essere evitate situazioni in cui si abbia abbagliamento diretto per la presenza di finestre, superfici luminose o lampade non schermate, nel campo visivo del lavoratore o anche abbagliamento indiretto per riflesso dovuto alla presenza di superfici lucide riflettenti (metalli, specchi, ecc.). Deve essere evitato anche l'abbagliamento per contrasto tra superfici illuminate e ambienti scuri (es. un segnale luminoso in un ambiente buio).

Si deve prevedere pertanto che le finestre siano munite di idonee schermature regolabili (tende, veneziane, frangisole, ecc.) e le fonti di luce artificiale devono essere provviste di schermi, esenti da sfarfallio e, possibilmente, con intensità luminosa regolabile. Sono da evitare anche la presenza di finestre o fonti di luce artificiale non schermate davanti ai monitor e lo schermo deve essere orientato ortogonalmente rispetto alle finestre.

Qualità dell'aria

Il livello della qualità dell'aria negli ambienti di lavoro deve essere tale da garantire la soddisfazione delle esigenze di benessere della maggior parte delle persone presenti nell'ambiente di lavoro e l'assenza di agenti inquinanti noti in concentrazioni tali da arrecare danno alla salute o causare condizione di malessere per gli occupanti.

Le principali fonti di inquinamento indoor sono l'uomo e le sue attività, i materiali da costruzione, gli arredi e i sistemi di trattamento dell'aria. In particolare, per migliorare la qualità dell'aria indoor e contrastare la nocività degli agenti inquinanti è opportuno adottare alcuni accorgimenti, quali assicurare un adeguato numero di ricambi d'aria, ottenuti anche attraverso la semplice apertura delle finestre per 5 minuti con intervalli di circa 2 ore. Negli ambienti in cui sono presenti impianti di ventilazione o di trattamento dell'aria è indispensabile venga effettuata la regolare pulizia dei filtri e delle bocchette di ventilazione.

Inoltre, è necessario verificare che le bocchette del trattamento dell'aria non siano ostruite da oggetti e che siano orientate in modo da impedire flussi d'aria diretti sulle persone.

Pulizia dell'ambiente

L'igiene degli ambienti di lavoro deve essere garantita da una corretta e regolare pulizia dei luoghi di lavoro evitando di fumare negli ambienti chiusi.

Microclima

Il microclima è il complesso dei parametri fisici che caratterizzano un determinato ambiente, i quali, insieme ai parametri individuali, quali l'attività metabolica e l'abbigliamento, determinano gli scambi termici tra l'ambiente stesso e gli individui che vi operano. Un microclima confortevole è quello che suscita nella maggioranza degli individui presenti, una soddisfazione per l'ambiente dal punto di vista termo-igrometrico, e quindi una situazione di "benessere termico" o "comfort". L'organismo umano è un sistema che opera in modo ottimale quando la temperatura del suo nucleo viene mantenuta entro un ristretto intervallo di variabilità (omeotermia), che si assesta tra i 36°C e i 37°C. Al fine del mantenimento della temperatura corporea fisiologica, l'organismo mette in atto dei meccanismi di termoregolazione stimolati da appositi sensori di caldo e di freddo (quali ad esempio, la sudorazione, la vasodilatazione, vasocostrizione, brividi, ecc.). Il benessere

termico si ottiene quando il raggiungimento dell'omeotermia avviene attraverso una fisiologica risposta del sistema di termoregolazione, e ciò si ha quando le condizioni microclimatiche sono confortevoli. Insufficienti condizioni microclimatiche nel luogo di lavoro, possono essere responsabili di malesseri vari (ad esempio in caso di esposizione diretta e prolungata a correnti d'aria) e raffreddamento (in caso di temperature troppo basse).

Al fine di prevenire il discomfort termico è necessario adeguare il vestiario alla temperatura degli ambienti e alle stagioni e assicurare livelli di temperatura e umidità conformi ai valori previsti dalle norme vigenti. In particolare, per le attività d'ufficio con la temperatura estiva: 19-24 °C (22 °C valore raccomandato) e con la temperatura invernale: 17,5 - 21,5 °C (19,5 °C valore raccomandato).

Per tutti i periodi stagionali è raccomandata un'umidità relativa compresa tra il 40% e 60%; Quindi è opportuno schermare le finestre con tende, ecc. e dotare gli impianti di termostati regolabili localmente. Provvedere anche alla regolare manutenzione e pulizia degli impianti di climatizzazione.

Rumore

Nell'ambiente di lavoro dove si utilizzano Videoterminali difficilmente sono presenti attrezzature particolarmente rumorose. Anche in presenza di una o più stampanti i livelli di intensità sonora non sono mai tali da provocare un danno all'apparato uditivo, tuttavia possono risultare fastidiosi per un'attività che può richiedere anche un'elevata concentrazione mentale e in particolare non devono perturbare l'attenzione e la comunicazione verbale.

Per contrastare il rumore in particolare si consigliano di installare i VDT in locali poco disturbati da fonti di rumore esterno e interno, scegliendo anche apparecchiature poco rumorose.

Rischio biologico da pandemia

In caso di situazione di questo tipo attenersi alle comunicazioni aziendali ricevute per lo stato emergenziale, alle ordinanze delle varie autorità competenti e comunque evitare luoghi affollati, locali pubblici, biblioteche, ecc. È preferibile e consigliato e spesso obbligatorio il lavoro dalla propria abitazione.

Check list di controllo dello smart worker:

Assicurarsi che il **luogo di lavoro prescelto** risponda ai seguenti requisiti:

- Verifica dell'efficienza ed integrità dei dispositivi e delle attrezzature prima dell'uso;
- Illuminato e areato naturalmente;
- Ben asciutto e difeso contro l'umidità;
- Condizioni adeguate di igiene;
- Pochi rumori che disturbano l'attività lavorativa;
- Per luoghi chiusi, ricambio d'aria garantito o da impianti di unità trattamento area o dalla presenza di aperture;
- Verifica dell'illuminazione e integrare se necessario con sistemi di illuminazione localizzata sui singoli posti di lavoro;
- In caso di lavoro al videoterminale, eliminare la luce diretta proveniente da finestre o da fonti artificiali non opportunamente schermate;
- Predisporre le proprie postazioni di lavoro in modo da evitare che i cavi e i collegamenti elettrici possano intralciare il passaggio e il normale transito delle persone, o possano essere sottoposti a danneggiamenti;
- Utilizzare un piano di lavoro che abbia preferibilmente le seguenti caratteristiche:

- Di colore opaco e non riflettente;
- Superficie sufficientemente ampia per disporre i materiali necessari e le attrezzature nonché consentire un appoggio per gli avambracci dell'operatore davanti alla tastiera, nel corso della digitazione;
- Profondità tale da assicurare una corretta distanza visiva dallo schermo; indicativamente fra 70 e 80 cm;
- Con uno spazio idoneo per il comodo alloggiamento e la movimentazione degli arti inferiori e per il sedile;
- Verificare che i tavoli e le scrivanie non abbiano spigoli vivi o parti usurate che potrebbero provocare tagli ed abrasioni;
- Utilizzare le apparecchiature di ufficio (personal computer, cuffie, telefoni cellulari ecc.) secondo le opportune modalità d'uso, verificandone in primis la stabilità sulle superfici di appoggio e la solidità dei sostegni (scrivanie, mobiletti);

In merito all'**impianto elettrico**, verificare che:

- Sia disponibile una dichiarazione di conformità o autocertificazione;
- Siano utilizzati, se necessari, adattatori e prolunghie adatti a supportare la corrente assorbita dagli apparecchi utilizzati;
- Assumere posizioni di lavoro corrette, adeguando la propria postazione e la disposizione delle apparecchiature abitualmente utilizzate in modo da evitare l'insorgenza di stati di affaticamento psicofisico e posturale;
- Premunirsi delle necessarie informazioni sull'adeguatezza ed il funzionamento degli eventuali sistemi di estinzione presenti e sui comportamenti da adottare e su come affrontare le eventuali situazioni di emergenza;
- Segnalare prontamente alla struttura aziendale eventuali anomalie o malfunzionamenti riscontrati nell'utilizzo delle attrezzature e non intervenire con arbitrarie operazioni di modifica del funzionamento o di riparazione, lasciando tali azioni al personale competente.

Informativa per il lavoratore:

Ribadiamo con la presente che il lavoratore che svolge la propria prestazione lavorativa in regime di "smart working", per i periodi nei quali si trova al di fuori dei locali aziendali, deve cooperare con diligenza all'attuazione delle misure di prevenzione predisposte dal datore di lavoro. Di seguito riportiamo alcune buone pratiche da seguire per evitare che si verifichino incidenti.

1. Assicurarsi dell'efficienza ed integrità dei dispositivi e delle attrezzature prima dell'uso.
2. Assicurarsi che il luogo di lavoro prescelto risponda ai seguenti requisiti:
 - a. Illuminato e areato naturalmente;
 - b. Ben asciutto e difeso contro l'umidità;
 - c. Condizioni adeguate di igiene;
 - d. Pochi rumori che disturbano l'attività lavorativa. Per luoghi chiusi, ricambio d'aria garantito o da impianti di unità trattamento aria o dalla presenza di aperture;
 - e. Integrare se necessario con sistemi di illuminazione localizzata i singoli posti di lavoro;
 - f. In caso di lavoro al videoterminale, eliminare la luce diretta proveniente da finestre o da fonti artificiali non opportunamente schermate.
3. Predisporre le proprie postazioni di lavoro in modo da evitare che i cavi e i collegamenti elettrici possano intralciare il passaggio e il normale transito delle persone, o possano essere sottoposti a danneggiamenti.
4. Utilizzare un piano di lavoro che abbia preferibilmente le seguenti caratteristiche:
 - a. Di colore opaco e non riflettente;
 - b. Superficie sufficientemente ampia per disporre i materiali necessari e le attrezzature nonché consentire un appoggio per gli avambracci dell'operatore davanti alla tastiera, nel corso della digitazione;

- c. Profondità tale da assicurare una corretta distanza visiva dallo schermo;
 - d. Stabile e di altezza, fissa o regolabile, indicativamente fra 70 e 80 cm;
 - e. Con uno spazio idoneo per il comodo alloggiamento e la movimentazione degli arti inferiori e per il sedile;
 - f. Verificare che i tavoli e le scrivanie non abbiano spigoli vivi o parti usurate che potrebbero provocare tagli ed abrasioni;
 - g. Utilizzare le apparecchiature di ufficio (personal computer, cuffie, telefoni cellulari ecc.) secondo le opportune modalità d'uso, verificandone in primis la stabilità sulle superfici di appoggio e la solidità dei sostegni (scrivanie, mobiletti).
5. In merito all'impianto elettrico, verificare che:
 - a. Sia disponibile una dichiarazione di conformità o autocertificazione;
 - b. Siano utilizzati, se necessari, adattatori e prolunghe adatti a supportare la corrente assorbita dagli apparecchi utilizzati.
 6. Assumere posizioni di lavoro corrette, adeguando la propria postazione e la disposizione delle apparecchiature abitualmente utilizzate in modo da evitare l'insorgenza di stati di affaticamento psicofisico e posturale.
 7. Ridurre al minimo movimenti rapidi e ripetitivi ed evitare di mantenere la stessa posizione per tempi prolungati.
 8. Premunirsi delle necessarie informazioni sull'adeguatezza ed il funzionamento degli eventuali sistemi di estinzione presenti e sui comportamenti da adottare e su come affrontare le eventuali situazioni di emergenza.
 9. Segnalare prontamente alla struttura aziendale eventuali anomalie o malfunzionamenti riscontrati nell'utilizzo delle attrezzature e non intervenire con arbitrarie operazioni di modifica del funzionamento o di riparazione, lasciando tali azioni al personale competente.
 10. Rischio biologico da pandemia
 - a. In caso di situazione di questo tipo attenersi alle comunicazioni aziendali ricevute per lo stato emergenziale, alle ordinanze delle varie autorità competenti e comunque evitare luoghi affollati, locali pubblici, biblioteche, ecc. È preferibile e consigliato il lavoro dalla propria abitazione.

4. STRUMENTI TECNOLOGICI E SICUREZZA DEI DATI

Testo redatto da **Dott. Gabriele E.A. Rossi, IT Innovation & Security Consultant - Aaron Technology**

Le **tecnologie** e le **connessioni** dati (fisse e mobili) odierne, entrambe sempre più performanti, hanno facilitato enormemente l'applicazione del lavoro a distanza. Tuttavia, il moltiplicarsi degli utenti e dei device che possono ormai connettersi da remoto a risorse interne all'azienda, ha obbligato le strutture informatiche ad abilitare sempre più "varchi" e modalità di accesso, complicando la gestione ed indebolendo il perimetro di **sicurezza** che protegge sistemi ed informazioni.

La sicurezza

Occorre allora porre particolare attenzione a non tralasciare il bisogno di protezione dei dati, che si manifesta in maniera "inversamente proporzionale" alla crescita di beneficio che tecnologia e connettività giorno dopo giorno fanno offrire.

In altre parole, **tecnologia** e **connettività**, quando sono performanti, risultano facilmente tatabili ed apprezzate dall'utente; la **sicurezza** no!

La sicurezza (quando c'è):

- lavora dietro le quinte, quindi l'utente comune non ha modo di notarne, od apprezzarne, la presenza;
- qualora richieda l'intervento dell'utente, essa complica e rallenta la maggior parte dei processi;
- quando fallisce, le alte performance di tecnologia e connettività agevolano in primo luogo le azioni fraudolente che il più delle volte riescono ad agire all'insaputa dell'utente, che (qualora se ne accorga) se ne accorge troppo tardi.

Di seguito due esempi su questo ultimo punto (ovvero quando la sicurezza fallisce) comparando gli effetti di connettività e tecnologie lente (di ieri) rispetto agli effetti di connettività e tecnologie più performanti di oggi:

effetti di connettività e
tecnologie lente (di ieri)

VS

effetti di connettività e tecnologie
più performanti (di oggi)

1. un tempo, una eventuale connessione non autorizzata ai propri sistemi, od un eventuale download del proprio database, rallentavano enormemente la rete, allarmando facilmente le vittime; oggi invece connessioni estremamente rapide possono consentire di lavorare in maniera eccellente da remoto, ma consentono anche a malintenzionati, una volta ottenuto un accesso, di scaricare (o caricare) quantità ingenti di dati da sistemi compromessi, senza che si manifestino effetti;

2. allo stesso modo, diversi anni fa, nel subire un attacco ransomware (ovvero subire la crittografia dei propri dati e dover poi pagare per riaverli) significava notare un incredibile rallentamento delle performance del proprio sistema; oggi, con le ottime performance di elaborazione e di scrittura su disco, un utente potrebbe accorgersene troppo tardi, lavorando senza problemi fino a quando il ransomware abbia già concluso la sua opera.

Tutto questo per dire che è fondamentale non fermarsi all'apparenza di una soluzione a prima vista efficace, ma occorre adoperarsi per verificarne (o farne verificare) e monitorare costantemente che sia vigente un'adeguata implementazione di sistemi di sicurezza e protezione.

Per chi ritenesse di non doversi preoccupare di difendere i propri sistemi, almeno una delle seguenti tre motivazioni è sempre presente e rende l'implementazione della sicurezza necessaria:

1. **difendere** il proprio **know how** interno ed i propri dati aziendali, che consentono di avere un vantaggio competitivo rispetto ai propri competitor (progetti, brevetti, informazioni di processo, clienti...);

2. **evitare** che i propri sistemi, una volta compromessi, diventino delle “**teste di ponte**” per l'archiviazione di materiale illegale e per la diffusione di software malevolo (in quest'ultimo caso è poi difficile provare di non essere complici);
3. **difendere i dati personali** delle persone fisiche interne ed esterne all'azienda, come richiesto anche dalle normative vigenti (Privacy e GDPR).

Il GDPR

Alla norma nazionale sulla Privacy (Decreto Legislativo 196/2003) si è recentemente aggiunto il Regolamento Europeo per la protezione dei dati personali (679/2016, altrimenti conosciuto come “GDPR”). In Italia queste due norme, per essere compatibili tra loro, hanno successivamente trovato un punto di incontro nel più recente Decreto Legislativo 101/2018.

La legislazione citata interessa i soggetti giuridici (comprese le partite IVA) che trattano all'interno dei loro sistemi e della loro struttura dati personali di qualunque persona fisica (in vita). Va da sé che praticamente ogni attività economica deve sentirsi coinvolta. Certamente il livello di sicurezza ambito occorre che sia proporzionato a:

- la qualità di dati personali coinvolti (ad es. i dati sanitari sono dati personali che richiedono attenzioni particolari);
- la possibilità di investimento della struttura.

In ogni caso conviene richiedere opportuna consulenza e la messa in atto delle soluzioni più coerenti a dei riferimenti qualificati.

È evidente perciò quanto valga la pena e quanto sia necessario adoperarsi attivamente per mantenere i propri sistemi in sicurezza.

Lo Smart Working

Il lavoro agile, ovvero il lavoro fuori sede o da remoto, aggiunge un importante grado di entropia a tutto quanto suddetto e moltiplica enormemente il fattore di rischio:

- le performance della tecnologia e delle connessioni devono essere prestanti sia presso la sede principale, sia presso il collegamento remoto;
- la sicurezza deve essere garantita:
 - presso i “varchi” della sede principale,
 - presso il device di connessione remota e
 - durante il tragitto che i dati percorrono.

Ribadendo pertanto la necessità di un'analisi dei rischi qualificata, si possono comunque individuare a grandi linee i bisogni tecnologici necessari, per ogni circostanza.

Riferendosi quindi allo Smart Working (relativamente al cosiddetto “lavoro al videoterminale”), la **dotazione necessaria** può essere sinteticamente individuata partendo principalmente da due elementi:

1. la **sorgente dati**, tipicamente digitale, su cui lavorare (come documenti, posta, database...);
2. un **complesso hardware e software**, quale computer, tablet, smartphone... abile ad elaborare la sorgente dati di cui sopra.

Non dimenticando che l'individuazione esatta della corretta strumentazione necessaria sia da identificare assieme al proprio riferimento IT o a seguito di una specifica analisi, una volta determinato da cosa sono rappresentati i due elementi all'interno della propria realtà, diviene possibile circoscrivere quanto altro occorre in maniera più dettagliata.

I dati

Qualora la sorgente dati da elaborare sia disponibile localmente, potrebbe essere semplicemente sufficiente uno strumento di elaborazione (del punto 2). Potrebbe essere ad esempio il caso di un autore di romanzi o trattati.

Qualora invece, come più di frequente, la sorgente dati sia formata da risorse condivise, remote od on line, quali documenti, posta, sistemi contabili o di gestione, diventa fondamentale un terzo elemento: la **connessione ad Internet**.

Internet

La connessione ad Internet è quindi condizione necessaria per accedere da remoto a **risorse** presenti **presso la propria sede lavorativa** o a risorse **in cloud**. Necessaria ma non sufficiente, poiché gli accessi alle risorse disponibili on line devono risultare protetti da sistemi di sicurezza e procedure di autenticazione che garantiscano:

- la protezione di eventuali dati personali trattati (come anche richiesto dalla legislatura),
- la protezione dei dati aziendali e
- l'accesso esclusivo ai soggetti incaricati.

In questo caso, se il proprio incaricato non sia in possesso di una propria connessione ad Internet, sarà necessario fornirgliela, se si desidererà metterlo in condizioni di poter operare in *smart working*. La tecnologia di oggi consente di scegliere tra diverse opzioni, anche economiche, per garantire una buona quantità di traffico dati ed una buona velocità.

Strumentazione

Allo stesso modo, il proprio incaricato dovrà essere in possesso di un *device* con caratteristiche coerenti (in termini di sicurezza e prestazioni) alla tipologia di elaborazioni da effettuare, altrimenti sarà necessario dotarlo anche della strumentazione necessaria.

Protezione

In particolare, la sicurezza verso le minacce, *esterne* alla propria organizzazione, è maggiormente garantita dall'utilizzo di *device* contenenti **sistemi operativi e software aggiornati alle ultime release**.

Le aziende più strutturate possono più facilmente permettersi di proteggere il proprio patrimonio informativo anche dalle minacce *interne*, **dotando i propri dipendenti di:**

- **tutti i device necessari** e
- della connessione per lavorare anche da remoto,

così da avere il pieno controllo della gestione e della protezione dei medesimi, potendone direttamente effettuare una corretta manutenzione e delimitarne l'uso per quanto occorre.

Si può optare infine per una soluzione mista in cui, utilizzando il proprio dispositivo grossomodo come un terminale, **ci si connette in remoto alla propria postazione** lavorativa e si lavora remotamente utilizzando esclusivamente la propria postazione locale per i dispositivi di input (es. tastiera e mouse) e di output (es. monitor).

Un accesso remoto alla propria sede aziendale prevede che siano stati configurati dei varchi di accesso e siano state pubblicate delle risorse che, seppur protetti nel migliore dei modi, **subiranno facilmente innumerevoli tentativi di accesso non autorizzati**.

Cloud

È proprio nel caso del lavoro da remoto che risulta indubbio il vantaggio pratico di avere le proprie **risorse** residenti **in cloud**, cosicché:

- possano essere **da dovunque raggiungibili**;
- buona parte delle criticità di sicurezza e di manutenzione da gestire siano delegate a servizi e fornitori esterni.

Manutenzione

È infatti stato verificato troppo frequentemente che (specialmente nelle piccole realtà) quando manutenzione e sicurezza sono a gestione interna, vengono lasciate a loro stesse fino all'avvenire di un incidente informatico: come ogni macchinario infatti anche il sistema informatico ha bisogno di un **continuo ed attento monitoraggio** del suo stato ed i pericoli a cui va incontro possono essere molto spesso invisibili fino a che non risulterà essere troppo tardi per intervenire. Si pensi ad esempio ad un contagio di tipo Ransomware, che spesso viene individuato solo quando i propri file sono già stati tutti crittografati e ormai non più accessibili.

Conclusioni

Organizzatevi pertanto con una figura interna dedicata od appoggiatevi a un'organizzazione esterna che vi consenta di operare in sicurezza, con riguardo particolare ai dati trattati, coerentemente con le vostre capacità di spesa.

Parimenti, per organizzare le proprie risorse umane a sessioni di lavoro da remoto, fate riferimento al vostro amministratore di rete e valutate insieme la soluzione tecnica ed economica migliore per voi.

5. ASPETTO ORGANIZZATIVO INTERNO ALL'AZIENDA

L'**adozione del modello di smart working** implica da parte delle aziende un enorme sforzo organizzativo in termini di:

- adozione di un nuovo paradigma culturale nella gestione del lavoro
- revisione dei processi di lavoro
- investimento tecnologico
- formazione dei dipendenti

I **lavoratori** devono imparare ad utilizzare strumenti di collaborazione innovativi e devono essere spinti ad assumere maggiore autonomia, oltre ad imparare a misurarsi sui risultati e a lavorare per obiettivi, quindi maggiore libertà legata a maggiori responsabilità.

L'**interazione a livello di team** è fondamentale, sono necessari confronti quotidiani attraverso piattaforme tecnologiche (Skype di Microsoft, Hangout e Meets di Google, Webex per Cisco, Zoom ecc) per migliorare produttività ed efficacia.

Il **nuovo modello di leadership manageriale** deve essere fondato su flessibilità e autonomia nella gestione degli orari, spazi e modalità di lavoro. È necessario lavorare sulla fiducia e sulla responsabilizzazione sui risultati.

Manager e Dirigenti devono fissare le modalità di svolgimento del lavoro, devono assegnare gli obiettivi e devono verificare che i dipendenti rispettino i vincoli (orario di lavoro, gestione ottimale dei rapporti con i clienti ecc.). Periodicamente devono monitorare e verificare i risultati che sono stati conseguiti e prendere provvedimenti per eliminare eventuali disfunzioni. Con strumenti tecnologici adatti è possibile condividere quotidianamente i lavori in modo che siano sempre facilmente accessibili.

I **Software di collaborazione aziendale** che servono ad agevolare la comunicazione tra i membri di un team, disponibili sul mercato, sono diversi. Sono strumenti che aiutano a **migliorare**

la condivisione delle attività aziendali: condivisione di file e report, di news e aggiornamenti, etc... Sono in grado di tracciare e salvare le varie discussioni, senza perderne la cronologia, come pure memorizzare tutte le modifiche apportate ai file condivisi da ogni membro. I più famosi software di Collaboration, sono Facebook Workplace e Microsoft Teams.

Siamo in un'epoca in cui **se non ti formi ti fermi**, per cui l'unica opzione è la formazione permanente. Videoconferenze e Webinar agevolano molto queste attività, ma bisogna positivamente constatare che la formazione è diventata negli ultimi anni un'attività accettata, ricercata e condivisa da tutti.

L'**azienda** per realizzare lo smart working deve lavorare sullo sviluppo di **infrastrutture e piattaforme digitali** adeguate a cui dipendenti e collaboratori possono facilmente accedere. **Serve una piattaforma aziendale in**



cloud dove caricare tutto il materiale da condividere. A livello strategico le organizzazioni devono lavorare sempre più per obiettivi e processi

Questo è un argomento particolarmente delicato perché fare scelte sbagliate in questo ambito può significare una perdita di terreno competitivo difficilmente recuperabile.

Riteniamo che lo Smart Working sia una modalità di lavoro da conoscere e da adottare nei casi opportuni, altresì riteniamo, da un punto di vista filogenetico, che l'interazione sociale sia alla base dello sviluppo umano. **L'uomo è un "animale sociale"**, privarlo dell'interazione sociale significa inserirlo in un processo di regressione fatale, lo smart working deve essere inteso come uno strumento estremamente utile da utilizzare, ma non va inteso come una finalità ultima del mondo lavorativo.

