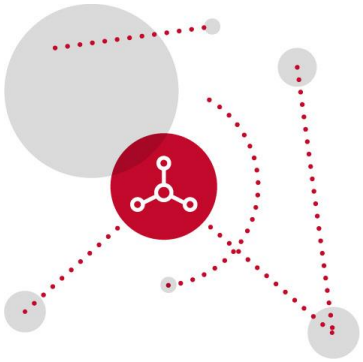
BonelliErede
with LOMBARDI

Focus Team Innovazione e Trasformazione Digitale
29 Maggio 2020

Lo "*smart working*" nell'emergenza Covid-19: utilità e rischi

Focus Team Innovazione e Trasformazione Digitale



Focus Team Leader
Tommaso Faelli
tommaso.faelli@belex.com
Tel. +39-02-771131

1. Introduzione

Fin dai primi giorni dell'emergenza sanitaria, **l'utilizzo dello *smart working (o "flexible work")* è stato individuato dal governo come una delle principali misure di contrasto alla diffusione del Covid-19**. Al fine di rendere più semplice il ricorso a questa modalità di svolgimento della prestazione lavorativa, i vari decreti emergenziali hanno introdotto alcune deroghe temporanee all'impianto normativo di base contenuto nella legge 81/2017, che ha introdotto il "lavoro agile" per i lavoratori dipendenti nel nostro ordinamento.

In questo momento storico è essenziale valutare con attenzione i profili di maggior criticità a cui i datori di lavoro devono prestare attenzione nel decidere di ricorrere a questa modalità di lavoro.

2. Lo "smart working" alla luce della normativa di emergenza: agevolazioni operative

La normativa di emergenza ha imposto lo *smart working* fin dal principio e, da ultimo, il DPCM del 25 febbraio scorso ha previsto la possibilità di accedere allo *smart working* anche in assenza di un accordo con i singoli lavoratori per tutta la durata dello stato di emergenza, ossia fino al prossimo 31 luglio.

Rimane fermo l'obbligo per il datore di lavoro di effettuare la comunicazione obbligatoria sul portale Cliclavoro entro 5 giorni dall'attivazione: tale obbligo può essere assolto mediante la procedura semplificata resa accessibile dal Ministero del Lavoro che consente il caricamento, con un unico flusso, di comunicazioni relative a più lavoratori.

Quanto all'obbligo, previsto dalla legge, di consegnare ai lavoratori in *smart working* un'informativa sui rischi generali e specifici connessi alla particolare modalità di esecuzione della prestazione, durante il periodo emergenziale, l'obbligo può essere assolto in via telematica (anche quindi con una semplice e-mail indirizzata ai dipendenti), utilizzando il modello di informativa resa disponibile sul sito dell'INAIL.

Autori

Marco Adda
marco.adda@belex.com
Tel. +39-02-771131

Tommaso Faelli
tommaso.faelli@belex.com
Tel. +39-02-771131

Vittorio Pomarici
vittorio.pomarici@belex.com
Tel. +39-02-771131

Vivian Grace Chammah
vivian.chammah@belex.com
Tel. +39-02-771131

Matteo Viani
matteo.viani@belex.com
Tel. +39-02-771131

Non mancano disposizioni rivolte a **particolari categorie di lavoratori**. Infatti, l'art. 39 del d.l. 18/2020 (c.d. decreto "Cura Italia", convertito in l. 27/2020) stabilisce che ai lavoratori del settore privato affetti da gravi e comprovate patologie con ridotta capacità lavorativa è riconosciuta la priorità nell'accoglimento delle istanze di svolgimento delle prestazioni lavorative in modalità agile.

Da ultimo, il d.l. 34/2020 (c.d. decreto "Rilancio") ha previsto, all'art. 90, che i genitori lavoratori dipendenti del settore privato che hanno almeno un figlio minore di 14 anni hanno diritto a fruire dello *smart working*, a condizione che nel nucleo familiare non vi sia altro genitore beneficiario di strumenti di sostegno al reddito in caso di sospensione o cessazione dell'attività lavorativa o che non vi sia genitore non lavoratore, e sempre che lo svolgimento dell'attività da remoto sia compatibile con le caratteristiche della prestazione lavorativa.

3. Il potere di controllo del datore di lavoro

L'utilizzo prolungato dello "*smart working*" genera inevitabilmente nel datore di lavoro la volontà - a volte l'esigenza - di controllare la qualità della prestazione resa dai propri dipendenti.

Il potere di controllo del datore di lavoro (anche sugli *smart workers*) è un aspetto estremamente delicato disciplinato fin dai tempi dello "Statuto dei Lavoratori" e va valutato di volta in volta alla luce delle caratteristiche della fattispecie specifica.

In via generale, è pacifico che al datore di lavoro sia riconosciuto il potere di controllare l'adempimento della prestazione lavorativa e di accertare eventuali mancanze dei dipendenti, anche ai fini dell'esercizio del potere disciplinare.

Lo Statuto dei Lavoratori (legge 300/1970, art. 4), come successivamente modificato, disciplina l'utilizzo di strumenti dai quali derivi "*anche la possibilità di controllo a distanza dell'attività dei lavoratori",* che, quindi, consentirebbero al datore di lavoro in qualunque momento di verificare il comportamento del lavoratore.

Fermo il divieto di installare o utilizzare strumenti - informatici o non - al solo scopo di controllare a distanza la prestazione lavorativa, lo Statuto dei Lavoratori (art. 4, comma 1) prevede che **gli strumenti da cui derivi "*anche la possibilità di controllo a distanza dell'attività dei lavoratori*" possono essere "*impiegati*":**

(i) ***"esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale"*** **e** a condizione che

(ii) l'installazione sia preceduta da un "***accordo collettivo*** *stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali*

aziendali" o, in mancanza di accordo o in assenza di rappresentanze sindacali, da un'autorizzazione dell'Ispettorato del Lavoro.

Ferma la necessità che sussistano effettive esigenze organizzative e produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale, il datore di lavoro è esonerato dall'obbligo di stipulare un accordo sindacale o di ottenere l'autorizzazione dell'Ispettorato, se lo strumento è "***utilizzat(o) dal lavoratore per rendere la prestazione lavorativa"*** o uno ***"strument(o) di registrazione degli accessi e delle presenze***".

Ferma l'eccezione degli strumenti di registrazione degli accessi e delle presenze, la giurisprudenza giuslavoristica definisce gli "strumenti di lavoro" sulla base del nesso funzionale esistente tra gli stessi e lo svolgimento della prestazione, ritenendo necessario verificare: "*se lo strumento affidato al lavoratore dal datore di lavoro sia* ***oggettivamente necessario all'esecuzione della prestazione lavorativa*** *e cioè se sia il mezzo utilizzato dal lavoratore per svolgere le sue mansioni*". Solo in questa ipotesi, non sarà necessario né l'accordo sindacale, né l'autorizzazione dell'Ispettorato del lavoro. È il caso di PC, *tablet*, cellulari, servizio di posta elettronica, collegamento a siti *Internet*.

Con una formula sintetica, ma molto efficace, il Garante ha affermato che rientrano negli strumenti di lavoro anche *"****le normali funzionalità degli apparecchi*** *forniti in dotazione, appunto, per rendere la prestazione*", ovverosia i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento.

Sono, invece, estranei alla definizione di strumenti di lavoro, gli *"****specifici sistemi modificativi dei dispositivi****, finalizzati al controllo personale del lavoratore".*

Con specifico riferimento al controllo del traffico *Internet*, non è stato considerato lecito dal Garante un trattamento di dati "*effettuato (…) per il tramite di* ***apparati (differenti dalle ordinarie postazioni di lavoro) e di sistemi software che consentono****, con modalità non percepibili dall´utente (c.d. in background) e in modo del tutto indipendente rispetto alla normale attività dell´utilizzatore (cioè senza alcun impatto o interferenza sul lavoro del dipendente),* ***operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" costanti ed indiscriminati degli accessi a Internet*** *o al servizio di posta elettronica*". "*Tali software*" - conclude il Garante – "*non possono essere considerati "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (ai sensi e per gli effetti dell´art. 4, comma 2, l. n. 300/1970*".

In senso conforme e con specifico riferimento al traffico Internet dei dipendenti, la giurisprudenza di merito ritiene che **le componenti che generano file di log e consentono operazioni automatiche di monitoraggio e di tracciatura degli accessi a Internet (o anche al servizio**

di posta elettronica) non possono essere considerate "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" ai sensi dell'articolo 4 comma 2, in quanto **possono esser considerati strumenti di controllo legittimi solo se finalizzati a realizzare una delle esigenze ivi previste (ad esempio, la maggiore sicurezza della rete aziendale) e solo se vi è il previo accordo con le OO.SS. o l'autorizzazione amministrativa**.

Lo statuto dei Lavoratori (art. 4, comma 3) prevede, poi, che le informazioni legittimamente raccolte "*sono* ***utilizzabili a tutti i fini connessi al rapporto di lavoro***", a condizione che al lavoratore sia data "***adeguata informazione*** *delle modalità d'uso degli strumenti e di effettuazione dei controlli*", nel rispetto della normativa in materia di trattamento dei dati personali. E' dunque di fondamentale importanza per l'azienda dotarsi di adeguate *policy* interne che disciplinino l'utilizzo dei mezzi informatici.

Ogni attività di controllo, comportando il trattamento di dati personali del dipendente, dovrà infatti essere posta in essere nel rispetto delle norme in materia di trattamento dei dati personali e delle indicazioni del Garante.

E' importante ricordare, infine, che la violazione delle previsioni sui limiti del potere di controllo del datore di lavoro è **passibile di sanzione penale**, ferme le conseguenze sanzionatorie - spesso molto onerose - per la violazione della normativa in materia di protezione dei dati personali (paragrafo seguente).

4. Tutela dei dati personali, cybersecurity e "Bring Your Own Device"

Il ricorso improvviso e massivo allo *smart working* come modalità di lavoro privilegiata durante l'emergenza sanitaria fa emergere anche nuovi punti d'attenzione per quanto riguarda la **tutela dei dati personali dei dipendenti** e la **tutela dei dati aziendali**.

Questa transizione repentina ha anche, in alcune realtà, creato l'esigenza di dotare di strumenti informatici mobili molti lavoratori che non si avvalevano di questa modalità prima dell'emergenza, portando talvolta a soluzioni basate sull'uso da parte dei lavoratori di propri dispositivi personali per rendere la prestazione lavorativa (modalità nota come "*Bring Your Own Device*"): tale soluzione è favorita anche dal decreto Rilancio, che all'art. 90 dispone che **la prestazione lavorativa in lavoro agile può essere svolta anche attraverso strumenti informatici nella disponibilità del dipendente** qualora non siano forniti dal datore di lavoro.
La decisione sulla possibilità di adottare la modalità *Bring Your Own Device* spetta al datore di lavoro, che dovrà effettuare questa scelta tenendo in conto, oltre alle esigenze organizzative, anche le esigenze di tutela dei dati personali e della riservatezza dei lavoratori, da una parte, e della sicurezza

e integrità dei sistemi aziendali e dei relativi dati dall'altra. Il datore dovrà, inoltre, tenere conto delle spese necessarie a dotare i dipendenti degli strumenti necessari a svolgere la prestazione da remoto: per andare incontro alle esigenze delle imprese, alcune Regioni, tra cui la Lombardia e il Lazio, hanno messo a disposizione dei **finanziamenti** per l'acquisto di strumenti tecnologici.

Attenuando la distinzione tra vita lavorativa e vita privata, lo *smart working* richiede da un lato una particolare attenzione a **evitare ingerenze nella sfera della vita privata del lavoratore**, mentre **sul piano della sicurezza dei dati** occorrerà tener conto di una situazione in cui da un lato viene meno l'apparato delle misure di sicurezza fisica normalmente adottate sul luogo di lavoro e dall'altro l'improvviso passaggio al lavoro da remoto per una gran parte della forza lavorativa mette sotto pressione reti e sistemi di sicurezza e modifica il panorama dei rischi cibernetici preesistente.

Sul piano del **diritto alla riservatezza e** della **tutela dei dati personali del lavoratore**, oltre a quanto richiamato nel paragrafo precedente sulla disciplina di eventuali strumenti che consentano un controllo anche indiretto sulle attività dei lavoratori, particolare centralità assumono le informazioni date ai lavoratori (per il mezzo di linee guida, *policy* o altre modalità) circa le regole di utilizzo degli strumenti lavorativi e il loro eventuale uso per finalità personali. Se per l'uso degli strumenti aziendali sono frequenti politiche aziendali che richiedano al lavoratore di contenere i propri appunti o documenti personali all'interno di aree di lavoro o cartelle personali, nel caso del *Bring Your Own Device* l'ottica sarà in qualche modo capovolta, essendo l'uso promiscuo del dispositivo non più un'eventualità, bensì la norma. Sembra, quindi, più coerente in questi casi ricorrere alla creazione, all'interno del dispositivo, di un'area apposita destinata agli applicativi e alle altre risorse usati per svolgere le attività lavorative, separando quest'area da quella destinata all'attività personale (c.d. *sandboxing*).

Anche sul piano della **tutela della confidenzialità, integrità e disponibilità dei dati e dei sistemi aziendali (*cybersecurity*)** è importante l'istruzione del personale circa i comportamenti da adottare per tutelare la sicurezza, quali ad esempio le procedure in caso di ricezione di comunicazioni sospette o di *data breach*. Una corretta risposta da parte del personale è, infatti, centrale soprattutto alla luce del notevole incremento delle attività malevole online (ad es. tentativi di *phishing*) che si è verificato nel corso dell'emergenza. Tuttavia, ancora più fondamentale per la tutela dei sistemi e dei dati aziendali è assicurare – anche, se necessario, attraverso una nuova analisi dei rischi e delle conseguenti misure da adottare – che l'impianto di misure di sicurezza organizzative e tecniche adottate dall'azienda sia adatto al nuovo scenario. Tra le principali raccomandazioni dell'ENISA relative al lavoro da remoto durante l'emergenza sanitaria (per ulteriori informazioni si veda il documento disponibile qui) vi sono:

- una particolare attenzione alle connessioni tramite VPN e ad assicurare che queste rimangano disponibili ed accessibili anche per

un numero di utenti molto maggiore rispetto al passato;
- l'uso esclusivo di canali di comunicazione criptati per l'accesso alle risorse aziendali;
- in caso di *Bring Your Own Device*, l'accertamento dell'idoneità dei dispositivi dal punto di vista della sicurezza informatica.

Se la necessità di assicurare il rispetto delle norme in materia di trattamento dei dati personali e di garantire la sicurezza di dati e sistemi con misure adeguate al livello di rischio riguarda qualsiasi organizzazione, particolare rilievo assume il rispetto di questi obblighi per quei soggetti identificati come "operatori di servizi essenziali" in base alla direttiva "NIS" (direttiva UE n. 2016/1148 "*recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*") o rientranti nel perimetro nazionale di sicurezza cibernetica ai sensi del D.lgs. n. 105/2019. Trattandosi di soggetti pubblici o privati "*da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato*" (art. 1 del D. lgs. n. 105/2019), la protezione della continuità operativa e della sicurezza dei dati e dei sistemi impiegati nello svolgimento delle loro attività è quanto mai cruciale nel contesto della crisi sanitaria.

5. Lo "*smart working*" alla luce dei principi di fiscalità internazionale

Lo svolgimento dell'attività lavorativa presso il domicilio personale dei lavoratori in regime di *smart working* e il blocco della mobilità tra Paesi può avere implicazioni di natura fiscale che devono essere attentamente considerate.

In talune circostanze, **lo svolgimento dell'attività da remoto può creare una dissociazione tra il Paese in cui viene svolta l'attività lavorativa e il Paese che beneficia di questa attività**. Questa situazione non è nuova nell'ambito dei gruppi multinazionali che adottano modelli organizzativi di tipo matriciale. Tali modelli organizzativi prescindono da una visione per *legal entity* e si caratterizzano per la presenza di funzioni chiave localizzate in un determinato Paese (che potrebbe essere diverso dal Paese in cui è localizzata la *legal entity* con cui il dipendente intrattiene il rapporto di lavoro) aventi responsabilità globali (è questo il caso, ad esempio, delle strutture articolate in *cluster* regionali).

Nelle predette situazioni occorre interrogarsi in merito alla possibilità che lo svolgimento dell'attività lavorativa da parte dei dipendenti che si trovano – per effetto delle misure governative di contenimento o in virtù della struttura del gruppo – in un Paese diverso da quello in cui risiede il soggetto che beneficia della loro attività lavorativa configuri l'esistenza di

una stabile organizzazione ("**SO**") – materiale o personale - di quest'ultimo nel Paese in cui si trova il dipendente[1].

Ai fini dello *smart working*, tale tematica rileva sia nella situazione in cui il lavoratore svolge la propria attività in Italia a favore di un datore di lavoro residente in un altro Paese (in questo caso si potrebbe configurare una SO in Italia dell'impresa non residente) sia nel caso in cui il datore di lavoro sia residente in Italia mentre il lavoratore svolge la propria attività in un altro Paese (in questo caso si potrebbe configurare una SO dell'impresa italiana nell'altro Paese).

A questo proposito, uno dei profili di rischio affrontati dall'OCSE nelle sue linee guida[2] riguarda proprio la potenziale emersione/creazione di SO legate al fatto che molte persone sono forzatamente relegate a lavorare da casa in modalità *smart working* per ordine dei rispettivi governi[3].

In proposito, l'OCSE ritiene che, in virtù dell'eccezionalità della situazione attuale, sia **improbabile che tali fattispecie conducano alla configurazione di una SO ("materiale" o "personale") nel Paese in cui si trovano i lavoratori.**

Le conclusioni cui giunge l'OCSE si basano sul fatto che (i) non vi sarebbe sufficiente grado di permanenza o continuità, (ii) l'impresa non avrebbe accesso o controllo sul luogo di svolgimento dell'attività lavorativa (*e.g.* la casa del lavoratore dipendente), e (iii) in normali circostanze il lavoratore avrebbe a disposizione uno spazio presso l'azienda per svolgere la sua attività.

In proposito va ricordato che la configurabilità di una SO "materiale" richiede, *inter alia*, un certo grado di permanenza (*degree of permanency*) ed essere a disposizione (*at the disposal*) di un'impresa. Proprio per questo, il fatto di **svolgere un'attività lavorativa da casa - in *smart working* - non determina automaticamente che tale luogo sia a disposizione del datore di lavoro.** Infatti, il *lockdown* è una misura temporanea e, dunque, inidonea a realizzare la condizione di permanenza richiesta dalla definizione di SO materiale. Inoltre, lo svolgimento dell'attività lavorativa in modalità *smart working* deriva da un'imposizione delle autorità governative e prescinde, quindi, da decisioni dell'imprenditore.

---

[1] Si potrà configurare una stabile organizzazione materiale in un Paese A di un' impresa residente in B nel caso in cui nel Paese A sia presente una sede (come, ad esempio, un ufficio) dell'impresa attraverso la quale viene esercitata in tutto o in parte l'attività economica propria di quest'ultima. Qualora, invece, a prescindere alla disponibilità di una sede, il dipendente, durante la permanenza nel Paese A concluda contratti per conto dell'impresa, allora vi può essere il rischio che esso dia vita ad una stabile organizzazione personale di questa.

[2] Il Segretariato generale dell'OCSE ha inoltre raccomandato che le amministrazioni finanziarie forniscano linee guida ai contribuenti (come già fatto da alcuni Paesi come, ad esempio, il Regno Unito, l'Australia e l'Irlanda).

[3] Il paragrafo 9 del documento pubblicato dal Segretariato generale dell'OCSE precisa che "…*it is force majeure not an enterprise's requirement*".

Sotto un concorrente profilo, si rileva che l'attività di un lavoratore dipendente che opera in qualità di agente dipendente per un'impresa non residente, in talune circostanze, può creare una SO "personale" dell'impresa non residente, qualora tale dipendente concluda abitualmente contratti o operi ai fini della conclusione degli stessi senza modifiche sostanziali da parte dell'impresa[4]. In tale circostanza, l'OCSE ritiene che tali attività, qualora siano svolte temporaneamente da casa (come ad esempio in *smart working*) a causa dell'attuale emergenza sanitaria e non rientrino nelle abituali attività del lavoratore dipendente, non creino i presupposti per la configurazione di una SO "personale". Diversamente, qualora le predette attività erano svolte (continuativamente) anche precedentemente all'attuale emergenza sanitaria, non si può escludere il rischio di SO "personale".

6. Conclusioni

L'inesorabile marcia dell'innovazione tecnologica ha ormai trasformato i modelli di business e il lavoro sempre più verso modalità di *smart working*.

L'esigenza di controllo del datore di lavoro è contemperata dalla tutela dei diritti del lavoratore e, pertanto, il potere del datore di lavoro è legittimato solo alle condizioni e secondo le modalità esaminate, in particolare potranno essere utilizzati solo strumenti effettivamente finalizzati a verificare obiettivi e livelli di produttività e non celino, invece, un mero controllo dell'attività del dipendente.

Nell'attuale scenario è necessario, infine, che le imprese eseguano attente procedure di *due diligence* interne volte ad esaminare le proprie strutture organizzative, l'opportunità di adottare "*tax control framework*", gli organigrammi e i rispettivi riporti, la contrattualistica afferente i rapporti di lavoro nonché i mansionari, in modo da ideare e attivare presidi che possano scongiurare l'emersione di rischi fiscali (tra i quali vi è l'emersione di SO).

[4] Tali contestazioni avvengono frequentemente laddove dipendenti di una società italiana svolgano tali attività in nome e per conto della società (solitamente appartenente al medesimo gruppo) non residente.

Focus Team Innovazione e Trasformazione Digitale

Il Focus Team è una costellazione di competenze in diversi ambiti di attività con focus su innovazione e trasformazione digitale.

Tommaso Faelli
Proprietà intellettuale

Marco Adda
Fiscale

Giulia Bianchi Frangipane
Societario

Alessandro Musella
Societario

Barbara Napolitano
Societario

Vittorio Pomarici
Lavoro

Maurizio Pappalardo
Antitrust

Federico Vezzani
Regolamentare

Gianpaolo Ciervo
Bancario