

Smart Working: alcune linee organizzative in ambito privacy

Webinar del 5 maggio 2020

Avv. Laura Priore

Iscritto all'Ordine degli Avvocati di Treviso, si occupa di consulenza legale alle aziende in ambito internazionale. Esperta nelle tematiche giuridiche in ambito privacy.

Humai
diritti e lib



COS'E' LO SMART WORKING



- La **Legge del 22 maggio 2017, n. 81** “Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato” **ha introdotto per la prima volta in Italia la formale regolamentazione del fenomeno dello Smart Working** o Lavoro agile.
- Si tratta di una **modalità di esecuzione del rapporto di lavoro subordinato** volta ad **“agevolare la conciliazione dei tempi di vita e di lavoro”** e in virtù della quale **le prestazioni possono essere rese** “in parte all'interno di locali aziendali e in parte all'esterno **senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale**” (art. 18, comma 1) **concrete modalità di esercizio sono demandate ad uno specifico accordo.**



LA DIFFUSIONE DELLO SMART WORKING A CAUSA DELL'EMERGENZA COVID 19

- **I vari decreti che si sono susseguiti nel corso dell'emergenza Covid 19, le successive circolari ministeriali e gli stessi Protocolli del 14.03.2020 – 24.04.2020 hanno previsto per i dipendenti delle aziende sia private che pubbliche la limitazione della presenza fisica dei dipendenti negli uffici ed una forma generalizzata di Smart Working, anche in deroga alla disciplina vigente da utilizzare per tutte quelle attività che possono essere svolte presso il domicilio.**
- **Le varie disposizioni non hanno però indicato gli adempimenti in termini di sicurezza dei dati personali** così anche la legge 81 del 2017 a parte un richiamo all'art. 4 dello statuto dei lavoratori.

NO A MISURE DI SICUREZZA «FAI DA TE»

- Dal punto di vista del trattamento dei dati personali lo Smart Working richiede:
 1. **Una preventiva analisi dei trattamenti coinvolti.** E' necessario **individuare** quali sono i dati personali trattati, le modalità con cui verranno trattati, da chi saranno trattati e soprattutto quali sono e possono essere i rischi sia per i lavoratori sia per l'impresa. Tale analisi può essere svolta con una procedura specifica regolamentata dal GDPR all'articolo 35.
 2. **L'attuazione ai sensi dell'art. 32 GDPR di misure tecniche ed organizzative per garantire un livello di sicurezza adeguato** al rischio, caso per caso, nel pieno rispetto della normativa vigente.
 3. **Rispetto dell'art. 4 dello statuto dei lavoratori** che disciplina **il divieto di mero controllo a distanza del lavoratore** se non in presenza di determinati motivi giustificativi e procedure attuative.

LA VALUTAZIONE DI IMPATTO



- E' una procedura prevista dall'art. 35 GDPR che mira a descrivere trattamento di dati per valutarne la necessità e la proporzionalità nonché relativi rischi allo scopo di approntare misure idonee ad affrontarli.
- «Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali».
- Sia per la norma sia per il garante tali presupposti richiedono di effettuare questa previa valutazione di impatto. Si veda [doc. web n. 905897] «trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti».

LE MISURE ORGANIZZATIVE

- **I dipendenti e collaboratori, già nominati autorizzati al trattamento, devono avere ricevuto precise istruzioni** relative al particolare trattamento dei dati fatto tramite lo smart working, l'azienda deve predisporre in ogni caso **una policy aziendale** con specifiche linee guida di comportamento;
- il datore di lavoro **deve rilasciare al lavoratore un'informativa aggiornata** ai sensi dell'articolo 13 GDPR circa i nuovi trattamenti effettuati mediante nuovi strumenti tecnologici;
- se il trattamento smart working richiede **l'utilizzo di fornitori esterni nuovi** che trattano dati per conto dell'azienda, questi fornitori devono essere **nominati responsabili del trattamento ai sensi dell'articolo 28 il GDPR**;
- se c'è una **procedura di data breach** questa va rinforzata rispetto ai nuovi rischi che effettivamente il la fuoruscita del dato dall' azienda può comportare (ex artt. 33 e 34 GDPR);
- inoltre una buona misura organizzativa è effettuare **la formazione dei lavoratori** con illustrazione delle linee guida adottate;



LE MISURE ORGANIZZATIVE: ESEMPIO DI POLICY AZIENDALE

- **regole in tema di utilizzo degli strumenti di lavoro** come per esempio l'obbligo di **utilizzare il dispositivo mobile aziendale solo ed esclusivamente per le attività lavorative**;
- **l'obbligo di individuare una stanza o comunque uno spazio deputato per allestire la postazione lavorativa** e che possa essere utilizzato in modo esclusivo durante il lavoro, anche di individuare un **luogo adatto ove riporre la documentazione e gli strumenti di lavoro** al termine della prestazione lavorativa;
- **il divieto di inserire nel dispositivo aziendale pennetta USB comunque basi dati esterne**;
- **il divieto di scaricare applicazioni non autorizzate** dall'azienda;
- **il divieto di postare o comunicare ai colleghi o a terzi le proprie credenziali** di accesso;
- **di comunicare al datore in modo preciso e puntuale gli orari di lavoro**;



LE MISURE ORGANIZZATIVE: ESEMPIO DI POLICY AZIENDALE

- **l'obbligo di chiedere** al datore di lavoro o all'amministratore di sistema, se presente, **l'autorizzazione per svolgere qualsiasi attività difforme** dalla policy. Il datore di lavoro deve garantire adeguate condizioni di supporto (assistenza nell'utilizzo delle apparecchiature, modulazione dei tempi di lavoro e delle pause);
- di **comunicare qualsiasi anomalia** informativa che viene riscontrata nel sistema durante la prestazione lavorativa;
- potrebbe poi essere consigliabile **predisporre un report periodico**;
- si devono infine **evidenziare le conseguenze disciplinari** delle violazioni di queste linee guida.

LE MISURE TECNICHE



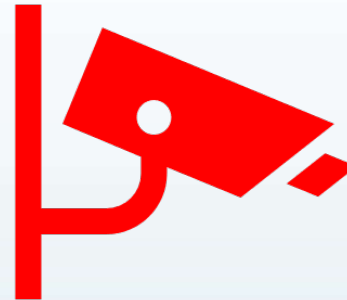
► Esigenza: creare uno spazio digitale protetto

Quello che **si richiede** è un **uso consapevole del digitale** anche nella scelta di strumenti adeguati. Le principali soluzioni potrebbero essere quella di:

- ricorrere a VPN quindi a reti virtuali private oppure ad ACL (liste di controllo degli accessi) per **limitare il rischio di accesso non autorizzato** di terzi al server aziendale
- Privilegiare l'uso di **dispositivi forniti dall'azienda**
- Adottare sistemi di **antivirus rinforzati**
- Standardizzare le **caratteristiche tecniche** dei dispositivi personali del lavoratore
- Creare un **profilo di accesso per** ogni singolo lavoratore.

Anche in questo caso l'azienda dovrà scegliere **le misure più adeguate al caso specifico**, per esempio in relazione al tipo di dati che tratta (particolarmente cosiddetti comuni).

IL CONTROLLO A DISTANZA (art. 4 Stat. Lav.)



- gli impianti audiovisivi e gli **altri strumenti dai quali derivi anche solo la possibilità di controllo a distanza dell'attività dei lavoratori** possono essere impiegati esclusivamente **per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale** e possono essere installati solo **previo accordo** collettivo stipulato dalle rappresentanze sindacali o, in mancanza, **previa autorizzazione** del competente Ispettorato del lavoro.
- Tale disposizione non si applica **agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa** ed agli strumenti di registrazione degli accessi e delle presenze.



IL CONTROLLO A DISTANZA (art. 4 Stat. Lav.)

- La prima riflessione è che gli strumenti tecnologici di cui abbiamo discusso prima, per esempio **sistemi di monitoraggio della navigazione in internet o della posta elettronica potrebbero costituire strumenti da cui derivi anche solo la possibilità di controllo a distanza** dell'attività dei lavoratori e quindi ricadere nella disciplina dell'art. 4.
- La seconda riflessione **è che è necessario individuare quali sono gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa che non devono essere autorizzati** secondo l'art. 4.
- Come da interpretazioni Ministero del Lavoro e delle Politiche Sociali – nota 18 giugno 2015 -, dall'Ispettorato Nazionale del Lavoro – circolare n. 2 del 7 novembre 2016 – e del Garante – provv. del 16 marzo 2017 **tali strumenti sono quelli indispensabili al lavoratore per adempiere la prestazione lavorativa messi a disposizione per tale finalità al lavoratore stesso.**



IL CONTROLLO A DISTANZA (art. 4 Stat. Lav.)

- Possono rientrare in questo ambito e non necessitare dell'autorizzazione per esempio **servizi, i software o gli applicativi strettamente funzionali alla prestazione lavorativa anche sotto il profilo della sicurezza.** A titolo esemplificativo possono essere considerati strumenti di lavoro **il servizio di posta elettronica offerto ai dipendenti mediante attribuzione di un account personale, gli altri servizi della rete aziendale fra cui anche il collegamento a sistemi internet ed i sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro.**
- **Non rientrano invece** tra gli strumenti indispensabili utilizzati dal lavoratore per rendere la prestazione lavorativa altri strumenti quali **i software che consentono con modalità non percepibili dall'utente per esempio in background operazioni di monitoraggio filtraggio, controllo e tracciatura costante indiscriminata degli accessi a internet o al servizio di posta elettronica da parte del lavoratore.**



IL CONTROLLO A DISTANZA (art. 4 Stat. Lav.)

- In ogni caso, nell'ambito dell'art. 4, le informazioni raccolte possono essere utilizzate solo se:
 - sia data al lavoratore **adeguata informazione** delle modalità d'uso degli strumenti e di effettuazione dei controlli (informativa e policy aziendale)
 - **il controllo sia sempre mantenuto in una dimensione umana** non esasperata dall' utilizzo di tecnologie che possono renderla continua ed anaelastica eliminando ogni zona di riservatezza e di autonomia nello svolgimento della prestazione



CONSIDERAZIONI

► LA DATA PROTECTION NON E' UN LIMITE MA UNA OPPORTUNITA'

E' necessario

- considerare che lo strumento dello smart working può essere uno strumento dell'era digitale adeguato per la competitività e per garantire le esigenze di conciliazione dei tempi di vita e di lavoro come menzionato nella legge 81 del 2017,
- la Data Protection non va vista come un limite a questo ma come un'opportunità per gestire al meglio una soluzione di questo tipo, come ogni altra soluzione aziendale.

GRAZIE PER L'ATTENZIONE!

Avv. Laura Priore – info@lpslegal.it – lpriore@bernardi.studio