SMART WORKING E PRIVACY:
OBBLIGHI DEL DATORE DI LAVORO E DELLO SMART WORKER

Lo *smart working*, che nel 2019 riguardava soltanto 570.000 lavoratori *(Fonte: Ministero del Lavoro e delle Politiche sociali)*, in pieno *lockdown* ha interessato circa sei milioni di dipendenti, ed a settembre, anche se il dato è ancora parziale, ne riguardava circa 4 milioni; si stima inoltre che il 58% di questi ultimi manterranno tale modalità lavorativa anche nel 2021 *(Fonte: il Sole24ore)*.

Davanti a numeri di questo genere, è purtroppo innegabile che la maggior parte delle aziende, in special modo le PMI, si sia rivelata severamente impreparata sotto svariati profili, tra i quali quello delicatissimo della tutela dei dati personali. E la medesima considerazione vale, seppur in misura minore, anche per i lavoratori agili.

1. SMART WORKING E COMPLIANCE DEL DATORE DI LAVORO AL REG. EU 679/2016 (G.D.P.R.)

Nell'ambito della *data governance*, l'implementazione del lavoro agile coinvolge tutta l'organizzazione aziendale poiché comporta un incremento di **responsabilizzazione** (c.d. "***accountability***") del datore di lavoro.

Il Regolamento impone infatti a quest'ultimo, quale titolare del trattamento, di riesaminare ed aggiornare le misure tecniche ed organizzative adottate qualora ciò si renda, come nel caso di specie, necessario (art. 24 G.D.P.R.) in ossequio al suddetto principio di *accountability* cui è improntato l'intero Regolamento Europeo n. 679/2016.

In quali adempimenti si traduce in pratica tale affermazione? Cosa deve fare il datore di lavoro? Di seguito, e senza pretesa di esaustività, un elenco dei principali adempimenti:

(i) **Analizzare e mappare i trattamenti**: significa individuare i nuovi trattamenti che vengono fatti in conseguenza del ricorso al lavoro agile, quali sono i dati coinvolti, da chi vengono trattati e come, con quali strumenti, quali sono le modalità di utilizzo dei medesimi dati e quali sono le istruzioni da fornire agli smart workers che li gestiranno.

Alcuni esempi pratici: il datore di lavoro attiva una VPN (*Virtual Private Network)* per il collegamento da casa per i dipendenti ai quali fornirà le credenziali per il *login*; dota i dipendenti di *devices* acquistandoli o noleggiandoli da terzi, oppure consente loro di utilizzare quelli privati (c.d. BYOID *Bring Your Own Device*), etc.

Questi e molti altri costituiscono **nuovi *asset*** che devono essere mappati, gestiti e regolamentati *ad hoc* attraverso l'analisi dei rischi che il datore di lavoro effettua con la c.d. **Valutazione d'impatto sulla protezione dei dati (D.P.I.A. Data Privacy Impact Assessment)** ex art. 35 G.D.P.R..

La D.P.I.A. è una procedura volta a descrivere uno o più trattamenti analoghi per natura, ambito, contesto, finalità e rischi, al fine di vagliarne **necessità, proporzionalità e rischi** onde adottare le idonee misure di sicurezza. Con la sua effettuazione il datore è *compliant* a quanto prescritto dal sopra citato art. 24 e dagli artt. 25 e 32 G.D.P.R.

(ii) **Integrare il Registro dei trattamenti** ai sensi dell'art. 30 G.D.P.R. con i nuovi elementi che riguardano le attività in *smart working* (trattamenti, banche dati, misure di sicurezza, *out sourcing,* etc.).

(iii) **Integrare l'Informativa** ex artt. 12 e 13 G.D.P.R. ai lavoratori agili in caso di eventuali nuovi trattamenti connessi a tale modalità di lavoro quale, ad es., il trattamento dei dati personali del lavoratore agile raccolti mediante l'utilizzo di strumenti di controllo - vedasi punto (v).

(iv) Predisporre **specifiche attività di formazione** tese a fornire allo *smart worker* i necessari strumenti di conoscenza e consapevolezza, unitamente alla predisposizione di specifiche ***policy*** o implementazione di quelle già esistenti, su cui anche formare gli stessi lavoratori.

(v) Valutare ai sensi del G.D.P.R. nel suo complesso e dello Statuto dei Lavoratori **l'eventuale potenziale invasivo di sistemi di monitoraggio della rete aziendale e dell'utilizzo dei devices.**

(vi) Verificare la conformità al G.D.P.R**. dei servizi, quali ad es. piattaforme, clouds, etc., forniti da terzi,** valutando la necessità di stipulare "*data processing agreement*" (art. 28 G.D.P.R.) o, se già in essere, la loro adeguatezza.

(vii) Predisporre, o implementare ove già esistente, **una procedura di *"data breach"*** (artt. 33 e 34 G.D.P.R.[1]) della quale i lavoratori agili devono essere **specificamente informati**, dovendo essi dare

tempestiva notizia al datore di lavoro qualora si verificasse una violazione di dati personali oggetto di trattamento, che ponga a rischio i diritti e le libertà della loro persona.

(viii) Garantire **la condivisione di files e contenuti** tra i lavoratori interessati tramite ***clouds*** particolarmente evoluti in termini di sicurezza.

(ix) Associare alle chiavi di sicurezza per l'accesso ai dati, **elementi ulteriori, quali ad esempio, apposite card token.**

(x) Assicurarsi che il dispositivo utilizzato dallo smart worker sia dotato di un **efficace software antivirus e antimalware.**

(xi) Effettuare periodicamente - e costantemente - il **back up delle informazioni**.

Fermo tutto quanto precede, è doveroso rilevare che a tutt'oggi la regolamentazione dello strumento in esame è in larga misura devoluta **all'accordo *one-to-one***, che rischia di violare i principi fondanti della L. 81/2017 e della normativa sulla protezione dei dati.

È pertanto auspicabile, nell'attesa di una normazione specifica ed unitaria da parte del legislatore, una contrattualizzazione privata del ricorso allo *smart working*, il cui contenuto sia il più chiaro e completo possibile.

2. IL LAVORATORE AGILE: COSA DEVE FARE E COME

Se il ricorso allo *smart working* ha notevolmente impattato sul datore di lavoro, altrettanto può dirsi con riguardo ai lavoratori.

Non vi sono norme specifiche da richiamare, piuttosto **condotte e cautele** da adottare che siano adeguate a tale modalità di lavoro e che dovrebbero essere state indicate dal datore di lavoro medesimo con apposita policy o codice disciplinare.

Condotte e cautele in linea di massima tutte orientate alla **vigilanza sulla sicurezza degli *end-point*, sul corretto uso della e-mail aziendale, sull'utilizzo esclusivo dei *devices*, sulla fruizione di connessioni sicure, sulla riservatezza dell'ambiente in cui si svolgono le mansioni.**

Vediamone, di seguito, alcune a mero titolo esemplificativo:

(i) predisporre all'interno della propria abitazione una postazione che consenta di lavorare in una **condizione di non contiguità con i familiari** e di **ridurre al minimo le interferenze di altri soggetti** eventualmente presenti all'interno dell'abitazione, anche in termini di rumore e/o ingerenze e distrazioni;

(ii) se **la rete utilizzata è domestica, verificarne la sicurezza** (no a collegamenti a reti pubbliche o in condivisione con uno o più vicini di casa)

(iii) proteggere i dati **contro rischi di distruzione e/o perdita, di accesso e/o trattamento non autorizzato** (non lasciando incustoditi, ad esempio, i dispositivi aperti e connessi);

(iv) utilizzare **solo strumenti ICT aziendali** (pc, tablet, smartphone…) concessi dal datore di lavoro in uso al di fuori dei locali aziendali solo per scopi lavorativi, e non anche personali (ad es. per consultare la propria e-mail personale o i propri profili social) o, in caso di utilizzo di pc personale, **creare un account protetto da password dedicato**;

(v) utilizzare **antivirus e antimalware** e aggiornarli costantemente;

(vi) effettuare frequentemente **un back office in ambiente offline**;

(vii) utilizzare **password sicure** (almeno 8 caratteri alfanumerici con segni di interpunzione) e **differenti per ogni ambiente di login, cambiandole spesso**;

(viii) effettuare **sempre il logout**;

(ix) fare molta attenzione ad **e-mail di provenienza dubbia**, contenenti *link* e/o allegati che non vanno mai cliccati e/o aperti ovvero con messaggi allarmistici (frequenti sono quelle di richieste di un piccolo aiuto economico a causa di una difficoltà contingente che si ricevono da un mittente presente tra i propri contatti, ma il cui è account è stato hackerato al fine di rubare la nostra identità –c.d. *phishing*-);

(x) **contattare il datore di lavoro e/o l'amministratore di sistema** per un qualsiasi dubbio, incidente o timore di incidente e/o violazione che possa compromettere la protezione dei dati personali (propri e/o di colleghi) e/o aziendali;

(xi) organizzare la giornata lavorativa **con orari il più possibile precisi** ed **attenervisi il più possibile** evitando o riducendo al massimo interruzioni per ragioni personali, e nel contempo prendersi le necessarie pause.

3. CONSIDERAZIONI CONCLUSIVE E UN ACCENNO AL DIRITTO ALLA DISCONNESSIONE

Svariati, come abbiamo visto, sono i profili di difficoltà che il massiccio e necessitato ricorso al lavoro agile ha comportato, sia dalla parte dell'azienda che da quella del dipendente.

Per quanto riguarda l'azienda, in estrema sintesi, far fronte agli obblighi, di cui innanzi si è fatta menzione, costituisce certamente adempimento ad obblighi di legge, ma altresì tutela del proprio business, ivi compresa **la c.d. *business continuity***, mediante l'incremento di impiego di risorse umane ed economiche nell'ottica di un crescente investimento in ICT (*Information and Communication Technology*).

Vi sono anche vantaggi sotto il profilo dell'organizzazione d'impresa in termini di riduzione delle postazioni di lavoro e minori costi generali di esercizio (energia, stampa, etc.), presenza di minor conflittualità interpersonale, etc.

Dal punto di vista del dipendente, numerosi i vantaggi, quali ad es. l'eliminazione dei tempi di spostamento e relativi costi, maggiore elasticità organizzativa, ma anche diversi gli svantaggi: considerevole riduzione della socialità, maggiore difficoltà nel reperire informazioni e quindi minore efficienza, e, ultimo, ma non per questo meno importante, il **c.d. effetto *"burn out"***.

Il *burn out,* letteralmente surriscaldamento, bruciatura o esaurimento, consiste in una condizione di disagio patologico rubricata dall'OMS tra i fattori che influenzano la salute nella *International Classification of Diseases* e che qui rileva in termini di psicopatologia del lavoro.

Alla base v'è una condizione di stress dovuta agli strumenti utilizzati dallo *smart worker* (ad esempio pc portatili e *smartphone*) che ne determinano una reperibilità ed una connessione, non solo potenziale ma di fatto, costante e continua, con conseguente compromissione del bilanciamento tra vita professionale e vita privata, che invece è tra le finalità dell'istituto del lavoro agile.

In questo quadro si inserisce **il diritto alla disconnessione,** ossia il diritto per il lavoratore di non essere costantemente online e quindi reperibile, e la libertà di non leggere e non rispondere alle comunicazioni di lavoro durante il periodo di riposo senza che a ciò determini la compromissione, anche parziale, della sua situazione lavorativa.

Il riconoscimento di tale diritto, nativo dei primi anni 2000 anche grazie ad una lungimirante giurisprudenza, è volto a tutelare il lavoratore ed in particolare quello agile da patologie che vanno, in ordine crescente di gravità, dal c.d. *tecno-stress* al sopracitato *burn out*.

Ci si limita, in questa sede, ai pochi accenni sopra indicati, trattandosi di argomento complesso e delicato che merita e richiede un approfondimento a sé, sia sotto il profilo normativo che giurisprudenziale.

Note

Riferimenti normativi

[1] Per "*data breach*" si intende quella violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Gli articoli 33 e 34 G.D.P.R. prevedono, rispettivamente, la notifica di una violazione dei dati personali all'autorità di controllo e la comunicazione di una violazione dei dati personali all'interessato.