LA PRIVACY NELLO SMART WORKING

scritto da goal | 27 Maggio 2022



di Stefano Bacchiocchi*

Con l'emergenza sanitaria si è assistito all'incremento forzato del lavoro in modalità agile.

La pandemia ha senza dubbio accelerato lo sviluppo e l'adozione dello smart working all'interno delle aziende e degli studi professionali.

Si tratta di un tema ormai travolgente per la vita delle imprese, visto l'esteso e crescente utilizzo delle tecnologie informatiche nel lavoro quotidiano; possiamo ormai dire che lo smart working è diventato una delle prassi lavorative più diffuse e ricercate dagli stessi lavoratori.

La legge 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*" all'art.18 ha previsto "il lavoro agile quale modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa".

A questa modalità lavorativa, si sono affiancati da subito anche i rischi di sicurezza informatica o di cybersecurity. Come conciliare quindi queste tecnologie con la privacy

e la protezione dei dati personali?

I controlli a distanza, da parte del datore di lavoro, sono leciti (nei limiti previsti dalla normativa) ma devono rispettare anche i principi del Regolamento Europeo in materia di trattamento dei dati personali, attenendosi ai principi di adeguatezza, correttezza e non eccedenza.

È quindi chiara la necessita dell'adozione di misure preventive volte alla protezione della riservatezza dei dati dei lavoratori, predisponendo anche delle valutazioni di impatto del trattamento che abbiano ad oggetto il bilanciamento degli interessi in gioco: da un lato il diritto del datore di lavoro di ottenere una prestazione lavorativa che non metta a rischio la struttura aziendale, dall'altro il diritto del lavoratore alla dignità, alla libertà personale e più in generale alla privacy e protezione dei dati personali.

Il punto focale della questione è che la prestazione lavorativa si svolge al di fuori dei locali dell'azienda, con tutte le conseguenze relative alla sicurezza nei luoghi di lavoro, al controllo da parte del datore di lavoro (controllo a distanza) e la sicurezza degli strumenti impiegati.

A questo si deve aggiungere che la strumentazione utilizzata dal dipendente potrebbe non essere strettamente aziendale ma, più realisticamente, impiegata anche in ambito familiare: ad esempio, si pensi alla rete wi-fi domestica, allo smartphone personale ecc., di fatto quindi fuori dal controllo diretto del datore di lavoro e potenzialmente meno sicura dal punto di vista informatico.

Uno dei maggiori problemi, infatti, riguarda l'utilizzo da parte dei dipendenti di dispositivi personali per connettersi alle attività aziendali da remoto. Questo fenomeno è il c.d. "Bring Your Own Device" che aumenta considerevolmente il rischio di problema o attacco informatico visto che tali device possono essere non conformi alle policy aziendali.

Le leggi applicabili in questo ambito sono principalmente, oltre alla già citata legge n. 81/2017, la legge 20 maggio 1970, n. 300 *"Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento"*, Statuto dei lavoratori, il GDPR e il decreto legislativo 10 agosto 2018, n. 101*"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".*

Il GDPR, in particolare, prevede che i titolari del trattamento (solitamente i datori di lavoro) debbano assicurare il rispetto della normativa mediante comportamenti concreti e documentabili. In altre parole, si devono giustificare le scelte compiute tramite documenti e relazioni scritte.

È opportuno quindi che il datore di lavoro adotti uno specifico regolamento interno che fornisca ai lavoratori le informazioni necessarie sull'utilizzo degli strumenti aziendali messi a disposizione, nonché la possibile attività di controllo in capo a quest'ultimo e una informativa chiara ed esaustiva, ai sensi dell'art.13 del GDPR, che contempli le modalità d'uso degli strumenti messi a disposizione, le caratteristiche di funzionamento, le regole per il loro utilizzo, le possibili modalità di controllo, quali dati saranno conservati e chi sarà autorizzato a trattarli, i tempi di conservazione e i provvedimenti disciplinari eventualmente previsti. In linea generale il trattamento deve rispettare i principi sanciti dal GDPR e pertanto le informazioni raccolte devono essere pertinenti, adeguate, non eccedenti le finalità per le quali sono state raccolte, necessarie, trasparenti e

limitate nel tempo.

Esistono strumenti tecnologici che aumentano la sicurezza informatica ma che incidentalmente causano un pervasivo controllo a distanza dei lavoratori: il ricorso a tali tecnologie non può rappresentare l'occasione per il monitoraggio sistematico del lavoratore.

Il controllo, infatti, deve avvenire nel rispetto delle garanzie sancite dallo Statuto a tutela dell'autodeterminazione del lavoratore, che presuppone anzitutto formazione e informazione dello Con l'emergenza sanitaria si è assistito all'incremento forzato del lavoro in modalità agile.

La pandemia ha senza dubbio accelerato lo sviluppo e l'adozione dello smart working all'interno delle aziende e degli studi professionali.

Si tratta di un tema ormai travolgente per la vita delle imprese, visto l'esteso e crescente utilizzo delle tecnologie informatiche nel lavoro quotidiano; possiamo ormai dire che lo smart working è diventato una delle prassi lavorative più diffuse e ricercate dagli stessi lavoratori.

La legge 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*" all'art.18 ha previsto "il lavoro agile quale modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa".

A questa modalità lavorativa, si sono affiancati da subito anche i rischi di sicurezza informatica o di cybersecurity. Come conciliare quindi queste tecnologie con la privacy

e la protezione dei dati personali?

I controlli a distanza, da parte del datore di lavoro, sono leciti (nei limiti previsti dalla normativa) ma devono rispettare anche i principi del Regolamento Europeo in materia di trattamento dei dati personali, attenendosi ai principi di adeguatezza, correttezza e non eccedenza.

È quindi chiara la necessita dell'adozione di misure preventive volte alla protezione della riservatezza dei dati dei lavoratori, predisponendo anche delle valutazioni di impatto del trattamento che abbiano ad oggetto il bilanciamento degli interessi in gioco: da un lato il diritto del datore di lavoro di ottenere una prestazione lavorativa che non metta a rischio la struttura aziendale, dall'altro il diritto del lavoratore alla dignità, alla libertà personale e più in generale alla privacy e protezione dei dati personali.

Il punto focale della questione è che la prestazione lavorativa si svolge al di fuori dei locali dell'azienda, con tutte le conseguenze relative alla sicurezza nei luoghi di lavoro, al controllo da parte del datore di lavoro (controllo a distanza) e la sicurezza degli strumenti impiegati.

A questo si deve aggiungere che la strumentazione utilizzata dal dipendente potrebbe non essere strettamente aziendale ma, più realisticamente, impiegata anche in ambito familiare: ad esempio,

si pensi alla rete wi-fi domestica, allo smartphone personale ecc., di fatto quindi fuori dal controllo diretto del datore di lavoro e potenzialmente meno sicura dal punto di vista informatico.

Uno dei maggiori problemi, infatti, riguarda l'utilizzo da parte dei dipendenti di dispositivi personali per connettersi alle attività aziendali da remoto. Questo fenomeno è il c.d. "Bring Your Own Device" che aumenta considerevolmente il rischio di problema o attacco informatico visto che tali

device possono essere non conformi alle policy aziendali.

Le leggi applicabili in questo ambito sono principalmente, oltre alla già citata legge n. 81/2017, la legge 20 maggio 1970, n. 300 *"Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento",* Statuto dei lavoratori, il GDPR e il decreto legislativo 10 agosto 2018, n. 101*"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".*

Il GDPR, in particolare, prevede che i titolari del trattamento (solitamente i datori di lavoro) debbano assicurare il rispetto della normativa mediante comportamenti concreti e documentabili. In altre parole, si devono giustificare le scelte compiute tramite documenti e relazioni scritte.

È opportuno quindi che il datore di lavoro adotti uno specifico regolamento interno che fornisca ai lavoratori le informazioni necessarie sull'utilizzo degli strumenti aziendali messi a disposizione, nonché la possibile attività di controllo in capo a quest'ultimo e una informativa chiara ed esaustiva, ai sensi dell'art.13 del GDPR, che contempli le modalità d'uso degli strumenti messi a disposizione, le caratteristiche di funzionamento, le regole per il loro utilizzo, le possibili modalità di controllo, quali dati saranno conservati e chi sarà autorizzato a trattarli, i tempi di conservazione e i provvedimenti disciplinari eventualmente previsti. In linea generale il trattamento deve rispettare i principi sanciti dal GDPR e pertanto le informazioni raccolte devono essere pertinenti, adeguate, non eccedenti le finalità

per le quali sono state raccolte, necessarie, trasparenti e limitate nel tempo.

Esistono strumenti tecnologici che aumentano la sicurezza informatica ma che incidentalmente causano un pervasivo controllo a distanza dei lavoratori: il ricorso a tali tecnologie non può rappresentare l'occasione per il monitoraggio sistematico del lavoratore.

Il controllo, infatti, deve avvenire nel rispetto delle garanzie sancite dallo Statuto a tutela dell'autodeterminazione del lavoratore, che presuppone anzitutto formazione e informazione dello stesso sul trattamento a cui i suoi dati saranno soggetti. È quindi assolutamente necessario intraprendere delle specifiche attività formative rivolte ai lavoratori da porre in smart working, affinché siano formati e informati sulle peculiarità di questo contratto. La violazione di tali principi comporterà delle conseguenze per i datori di lavoro inadempienti.

Si ricorda, inoltre, che Privacy significa anche protezione dei dati personali e delle informazioni aziendali e, a tal fine, la normativa privacy/GDPR impone al titolare del trattamento di adottare misure tecniche ed organizzative adeguate a garantire la sicurezza dei dati. È opportuno quindi adottare una serie di accorgimenti utili a tal fine. In questo senso, in un ambiente lavorativo sempre più votato all'informatica ed alla digitalizzazione dei sistemi e dei processi, è opportuno nominare formalmente il c.d. Amministratore di Sistema.

L'amministratore di sistema è una figura con specifiche competenze su hardware e software, soprattutto per quanto riguarda le caratteristiche delle architetture informatiche, dei gestionali d'impresa e delle reti di comunicazione.

Nel mondo informatizzato ormai anche questa figura si è evoluta dal tipico "tecnico del computer" ed è normale oggi

che negli ambienti di lavoro ci siano più interlocutori diversi: chi gestisce la rete, chi i computer, chi le stampanti, chi i telefoni, chi il gestionale di studio, chi le piattaforme online ecc.

Oltre a ciò, queste figure spesso si occupano della gestione informatica a tutto tondo: architettano sistemi di backup e attività di disaster recovery, organizzano la gestione dei dati informatici, sorvegliano il buon andamento dei flussi documentali, ecc.

In ottica di fornire qui alcune indicazioni pratiche si ritiene di sconsigliare l'utilizzo di dispositivi personali dei lavoratori, ricorrendo invece preferibilmente a dispositivi forniti dall'azienda. I dispositivi adottati dovranno essere dotati di un buon antivirus, di un sistema di backup, di cifratura dei dati e connessione protetta.

Per l'accesso ai sistemi aziendali da remoto, si consiglia almeno di utilizzare un sistema di autenticazione a due fattori (quindi non il semplice sistema basato su password).

La normativa privacy prevede espressamente che si debbano trattare dati attraverso precisi profili di autorizzazione; di conseguenza, il lavoratore in remoto deve poter accedere e trattare solo i dati di sua competenza.

Un ulteriore adempimento obbligatorio è l'aggiornamento del cd. Registro Dei Trattamenti con lo scopo di elencare tutti i trattamenti effettuati e i relativi dati personali utilizzati e/o trasferiti a terzi. Questo documento, se opportunamente redatto, permette di avere una panoramica completa di tutte le informazioni personali che si trattano abitualmente; è quindi un ottimo punto di partenza per riuscire a studiare e coordinare i metodi di difesa.

La normativa ha previsto inoltre che il datore di lavoro debba studiare attentamente una procedura da attivarsi se, nonostante tutti i sistemi di difesa adottati, si verifichi

ugualmente il c.d. Data Breach.

Questa terminologia indica un incidente di sicurezza durante il quale i dati personali di persone fisiche vengono trattati, consultati (o rubati) ecc. da soggetti non autorizzati. In altre parole, è un evento non programmato che intacca l'integrità e correttezza dei dati personali trattati o il loro grado di riservatezza.

È opportuno, inoltre, che il datore di lavoro si affretti a predisporre, (in ottica di accountability e, eventualmente, per obbligo di legge), qualora non sia già stato fatto, la redazione della c.d. DPIA (Data Protection Impact Assessment): di fatto una descrizione dei rischi dell'adozione dello smart working e delle misure scelte per mitigarli.

Possiamo qui riassumere i requisiti minimi per rispettare (almeno per la parte documentale) la normativa citata: aver preparato un'informativa privacy esaustiva, avere adottato un registro dei trattamenti, avere effettuato la valutazione di impatto (DPIA) per quei trattamenti che la richiedono, avere adottato un protocollo per reagire al data Breach in modo tempestivo.

Ricordiamo inoltre che, nella maggior parte dei casi, gli attacchi informatici che hanno successo sono causati da un errore umano. Infatti spesso si sottovaluta il rischio di un problema o attacco informatico che viene considerato (erroneamente) improbabile. È quindi fondamentale, ed obbligatoria, la formazione puntuale e documentabile dei dipendenti/collaboratori.

Infine, ricordiamo che per aiutare i datori di lavoro a pianificare le operazioni (ed anche evitare le salatissime sanzioni) la normativa prevede fortunatamente una nuova figura in ambito privacy l'RPD (Data Protection Officer – DPO), con funzioni che vanno dalla sorveglianza dell'applicazione del GDPR alla promozione della cultura della tutela dei dati

personali, fino alla gestione dei rapporti con l’Autorità Garante; il DPO è quindi una sorta di “revisore” dedicato alla privacy.

In sintesi, la normativa impone un obbligo al datore di lavoro che dovrà verificare se le soluzioni tecnologiche messe a disposizione dei dipendenti/collaboratori siano conformi alla normativa e dovrà valutare quindi (insieme al DPO, se nominato) l’effettiva adeguatezza delle misure tecniche ed organizzative messe in campo.

**Odcec Brescia*