CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

SMART-WORKING AGEVOLATO: TRA BUSINESS CONTINUITY E GARANZIE LEGALI A PRESIDIO DELLA RISERVATEZZA DEL LAVORATORE E DEL KNOW-HOW AZIENDALE

Il contributo si propone di illustrare le specificità connotanti il necessitato ricorso a policies lavorative "agili", da parte di aziende e P.A., in considerazione delle peculiari deroghe – introdotte con DPCM del 4 marzo 2020 (recante disposizioni attuative per il contenimento e la gestione dell'emergenza epidemiologica da Covid-19) – semplificative rispetto alla disciplina istitutiva del lavoro in modalità flessibile (contenuta nella l. n. 81/2017, c.d. Jobs Act autonomi).

di **Gianpiero Gaudiosi**
IUS/07 - DIRITTO DEL LAVORO
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Venerdì 3 Aprile 2020

CamminoDiritto.it
ISSN 2421-7123

Sommario: 1. Brevi cenni storici. Uno sguardo all'illustre predecessore: il telelavoro; 2. Inquadramento concettuale del lavoro agile e normativa di riferimento; 3. Quali i rischi per la privacy dello smart-worker?; 3.1 Poteri datoriali di controllo. Analisi delle deroghe introdotte dalle misure governative emergenziali; 4. Obblighi del lavoratore a tutela dei segreti aziendali. Spunti conclusivi.

1. Brevi cenni storici. Uno sguardo all'illustre predecessore: il telelavoro

In concomitanza con la repentina evoluzione del paradigma tecnologico e con la capillare diffusione degli strumenti informatici connessi in rete, è già agli albori del nuovo secolo che trovano collocazione i primi studi preordinati a incentivare il telelavoro (all'epoca anche conosciuto con i termini di telework o eWork). Sebbene la paternità dell'idea di de-materializzare il lavoro affondi le sue radici negli scritti di Jack Nilles (che, nei primi anni '70, coniò il concetto di telecommuting o telependolarismo), fu con il progetto Teldet (1996) ed il progetto EcaTT (2000) - ambedue fondati e commissionati dalla Comunità europea – che si ipotizzò una concreta applicazione su ampia scala di tale innovativa strategia lavorativa, in ragione dei benefici rivoluzionari che avrebbe potuto apportare alla struttura socio-economica dei Paesi comunitari. Ciò malgrado, la flebile crescita dell'economia globale nei territori europei - sedi di una soltanto preannunciata rivoluzione epocale nel modo di concepire il lavoro – costituì il risultato di una timida risposta agli esiti dello sviluppo di un siffatto modello. Tale evidenza empirica rifletteva un dato in origine trascurato dagli studi di settore: si trattava di sperimentazioni imperniate su un radicale ripensamento della competitività delle imprese - in quanto strettamente condizionata dalle loro capacità di accesso alle tecnologie informatiche - e sull'idea rivoluzionaria di sviluppo sostenibile (come definito, per la prima volta, dalla Commissione Brundtland nel 1987), in ragione delle molteplici esternalità positive che sarebbero derivate dalla delocalizzazione del lavoro (dalla riduzione dell'inquinamento alla minore pressione antropica in aree particolarmente congestionate). In definitiva, al vaglio di tempi immaturi, il modello non rispettò da subito le attese sperate.

2. Inquadramento concettuale del lavoro agile e normativa di riferimento

Detti brevi cenni storici[1] costituiscono il preludio indispensabile per approcciare correttamente al concetto anglosassone di smart working e alla relativa traduzione italiana di "lavoro agile" (ma anche efficiente, organizzato). Si tratta di termini oggi tornati in auge per descrivere la prassi su cui massicciamente ripiegano le aziende e le pubbliche amministrazioni allo scopo di contemperare le relative esigenze di continuità operativa e/o produttiva con le stringenti limitazioni ai diritti essenziali (tra tutti, in particolare per i lavoratori, assume rilievo quello ad una libera circolazione ed allo spostamento nel territorio nazionale), motivate dall'epidemia di Coronavirus. Seppure la parola inglese, di

CamminoDiritto.it
ISSN 2421-7123

più recente conio, sia impropriamente usata quale sinonimo della risalente idea di "telelavoro", si tratta di modelli concettualmente distanti. Se, da un lato, l'"antenato", ossia il telelavoro, si proponeva di trasferire la prestazione lavorativa dal chiuso degli uffici aziendali verso postazioni ben definite (comunemente l'abitazione del lavoratore), a parità di regole sui tempi, nonché con orari rigidamente imposti (secondo un modello tecno-centrico, teso a valorizzare l'apporto reso dalle strumentazioni tecnologiche), al contrario, lo smart-working individua una modalità flessibile di esecuzione del lavoro, finalizzata a promuovere la produttività ed efficienza del lavoratore, collocando le tecnologie su un piano strumentale (l'impiego delle quali garantisce un'universalizzazione dei luoghi di adempimento della prestazione lavorativa, slegata da una rigida articolazione degli orari). In ambito nazionale, il modello di smart working – perciò utile a identificare, come poc'anzi anticipato, non già un rinnovato schema di contratto, quanto piuttosto una logica organizzativa incentrata sulla qualità del quomodo e non sulla misurazione del quantum di esecuzione delle prestazioni in regime di lavoro subordinato – rinviene il principale e più recente referente normativo nel testo delle disposizioni contenute nel Capo II della Legge del 22 maggio 2017, n. 81. La citata legge, recante le "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" si applica anche ai lavoratori del pubblico impiego, come chiarito ai sensi dell'art. 3 ("le disposizioni (del Capo II) si applicano, in quanto compatibili, anche nei rapporti di lavoro alle dipendenze delle amministrazioni pubbliche").

3. Quali i rischi per la privacy dello smart-worker?

Compreso l'impatto positivo che l'implementazione dell'impiego di lavoratori smart è in grado di apportare nel settore privato alle imprese (da una maggiore flessibilità organizzativa che passa attraverso l'aumento del tasso di produttività del singolo lavoratore sino alla riduzione delle spese interne legate ai benefits), e in quello pubblico (mediante il miglioramento e l'offerta di servizi pubblici capillari al cittadino), si pongono, tuttavia, una serie di questioni di non secondario rilievo. La prima questione interseca il più elevato rischio di violazione, in danno dei lavoratori, della normativa dettata a tutela della protezione dei dati personali (oggi, Reg. EU 679/2016, c.d. GDPR, e corrispondente adeguamento nazionale con d. lgs. n. 101/2018) che viene concretandosi in conseguenza della obbligata scelta, da parte delle imprese, di ricorrere ad una gestione in modalità smart di compartimenti essenziali per garantirne la c.d. business continuity. Si tratta di un rischio di cui si fece precorritore, già nel 2018, l'allora Garante europeo della protezione dei dati, Giovanni Buttarelli, tra le cui parole in particolare si legge: "La possibilità che esigenze di sicurezza o produttive possano comportare un controllo a distanza come effetto secondario del controllo stesso è divenuta in molti contesti la regola, anziché l'eccezione. In altre parole, le moderne attività lavorative comportano, per default, un monitoraggio capillare dei più minimi dettagli delle attività stesse"[2]. E poiché

CamminoDiritto.it
ISSN 2421-7123

nel contesto odierno, la stragrande maggioranza delle attività lavorative va reinquadrata, per forza di cose, in un ambiente digitale, occorre definire con precisione i confini entro i quali possa trovare estrinsecazione l'esercizio del potere di controllo del datore sulla prestazione resa dal lavoratore all'esterno dei locali aziendali.

3.1. Poteri datoriali di controllo. Analisi delle deroghe introdotte dalle misure governative emergenziali

Trattandosi di lavoratori che operano da remoto, il controllo a distanza potrebbe, prima facie, apparire strettamente necessario e tale da richiedere l'impiego di software e programmi che "riducano le distanze". Argini all'attività di controllo a distanza sembrano essere stati definiti, a monte, dal legislatore con l'art. 21 della legge n. 81, citata, che abilita l'accordo individuale (c.d. "di lavoro agile") a regolare l'esercizio di detto potere, nel rispetto di quanto stabilito dall'art. 4 dello Statuto dei lavoratori (che, a sua volta, stabilisce che l'installazione di impianti audiovisivi e strumenti dai quali possa derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori avvenga previo accordo sindacale ovvero di autorizzazione amministrativa proveniente dall'Ispettorato Nazionale del Lavoro). Accordo in relazione al quale, tuttavia, come previsto dalla normativa emergenziale (DPCM 4 marzo 2020[3]) – nell'ottica di indicare una procedura semplificata rispetto alla disciplina istitutiva – è ammessa una deroga, per l'intera durata dello stato di emergenza nazionale, relativamente alla necessità che esso sia sottoscritto con ogni singolo collaboratore. Inoltre, in ipotesi di sottoscrizione di accordi individuali in numero elevato, è stata introdotta la possibilità per l'azienda di effettuarne la comunicazione in forma massiva, per via telematica, specificando eventualmente il riferimento al sopra menzionato DPCM.

La principale novità apportata dalla norma contenuta all'art. 21, introduttiva del c.d. "accordo agile" o anche detto "one-to-one", era stata sostanzialmente riscontrata nella scelta, da parte del Legislatore, di coinvolgere – valorizzando ancora una volta la flessibilità spazio-temporale del lavoro agile – il lavoratore nella definizione delle suddette modalità di controllo, attraverso un accordo che si inserisce in un'ottica esclusivamente migliorativa della posizione dello smart worker, e limitando contestualmente (senza però comprimere del tutto) l'esercizio del corrispondente potere datoriale.

A fronte di questo intento del Legislatore, ci si era chiesti, altresì, come andasse a conciliarsi con la ratio dell'art. 21 l'eccezione di cui all'art. 4 comma 2 (cui la norma fa rinvio), che sembrerebbe esentare il datore dall'obbligo di rispettare la procedura codeterminativa (di cui al co. 1 della medesima disposizione) quanto "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa". In giurisprudenza è

CamminoDiritto.it
ISSN 2421-7123

sembrata prevalere la tesi secondo la quale l'eccezione di cui all'art. 4 St. lav. andrebbe interpretata stricto sensu, visto l'atteggiamento di favore mostrato dal legislatore, in considerazione delle peculiarità del rapporto di lavoro de quo; inoltre, attesa la fisiologica debolezza contrattuale del lavoratore, è stata riconosciuta la necessità di evitare la stipulazione da parte del dipendente di accordi lesivi dei suoi diritti fondamentali (quale quello alla riservatezza dei suoi dati personali) ben oltre le ragioni rese necessarie dalla funzionalità del rapporto[4].

Per vero, tale quadro normativo - ispirato da una logica di favor per la peculiare posizione dello smart worker - non può ritenersi affievolito dalle summenzionate misure derogatorie, in quanto va egualmente letto alla luce dell'art. 115 Codice della Privacy, che sancisce l'obbligo in capo al datore di lavoro di garantire, in ogni caso, il rispetto della personalità e della libertà morale del lavoratore agile. Per tale ragione, sono da ritenersi sempre vietate (anche alla luce delle posizioni recentemente assunte dal Garante Privacy) tutte le attività che si concretizzino in un monitoraggio costante ed indiscriminato del dipendente. Una tale previsione, di carattere generale oltreché omnicomprensiva dei rischi di lesione ai quali il lavoro smart potrebbe esporre la privacy del lavoratore, ledendone la libertà di autodeterminazione personale e professionale, obbliga il datore a predisporre una policy aziendale, da cui risulti l'indicazione: a) degli strumenti aziendali forniti, che consentono il controllo a distanza; b) delle relative modalità e regole di utilizzo (in particolare, per quanto riguarda l'utilizzo della posta elettronica e di internet); c) delle modalità, dell'oggetto e della frequenza dei controlli cui sono sottoposti i lavoratori a distanza; d) dei dati conservati e delle relative modalità di conservazione, nonché dei soggetti abilitati ad accedervi; e) infine, circa i rischi connessi alle particolari modalità di esecuzione del lavoro a distanza.

È, inoltre, richiesto che tale policy venga sottoposta a costanti aggiornamenti periodici da parte del datore di lavoro. Ciò è conseguenza, altresì, di quanto esplicitato all'art. 22 della legge n. 81/17, a tenore del quale il datore ha il dovere di garantire la salute e la sicurezza del lavoratore che svolga la prestazione in modalità di lavoro agile; dovere che si traduce, quindi, in uno specifico obbligo di consegnare al lavoratore "con cadenza almeno annuale, un'informativa scritta nella quale sono individuati i rischi generali e i rischi specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro". Sul punto, la normativa emergenziale di semplificazione e incentivazione del lavoro agile ha previsto che sia consentito ai datori di lavoro l'assolvimento degli obblighi previsti dal citato articolo 22 in via telematica, ricorrendo alla documentazione resa disponibile sul sito dell'Istituto nazionale assicurazione infortuni sul lavoro (INAIL). Orbene, indipendentemente dalle modifiche imposte dalla situazione di emergenza, in virtù della disciplina contenuta nel nuovo codice della privacy, resta fermo che il trattamento dei dati personali dello smart worker debba sempre rimanere assoggettato a tutta una serie di principi generali (da quello di proporzionalità alla trasparenza del trattamento).

CamminoDiritto.it
ISSN 2421-7123

Perfettamente in linea con tali criteri è apparsa, altresì, la possibilità da parte del datore di applicare ai propri dipendenti le tecniche di geolocalizzazione (tramite localizzazione dei dispositivi affidati al personale in servizio all'esterno). Come da recenti posizioni assunte dal Garante per la protezione dei dati personali, è opportuno però che siano rispettati dal datore accorgimenti a tutela degli interessati, "come la necessità di configurare il sistema in modo da impedire il trattamento di dati ulteriori e non pertinenti rispetto alle finalità indicate (in particolare dei dati relativi al traffico telefonico, agli sms, alla posta elettronica, alla navigazione in internet)"; inoltre, quando l'applicazione lavora in background, è imposto all'azienda di programmare un sistema in grado di prevedere un'icona indicante che la funzione di localizzazione è attiva[5]. In ipotesi in cui il lavoratore non sia stato adeguatamente e correttamente informato in merito alle modalità d'uso degli strumenti ed effettuazione dei correlati controlli, nel rispetto di quanto previsto dal Codice Privacy, è prevista la inutilizzabilità assoluta dei dati raccolti.

4. Obblighi del lavoratore a tutela dei segreti aziendali. Spunti conclusivi

Per concludere, a carico del datore di lavoro è imposto l'obbligo di adottare un insieme di misure tecniche idonee a prevenire la perdita o la dispersione dei dati personali del lavoratore (data breach), a salvaguardia della sua privacy. Tale dovere, d'altronde, si configura anche in ragione dell'interesse alla conservazione dei segreti aziendali. Sotto questo secondo profilo vengono in rilievo una serie di obblighi che fanno capo oltre che al datore di lavoro, anche al singolo lavoratore, che svolge le sue mansioni da casa, il più delle volte sprovvisto di specifiche competenze in materia di cyber security. In considerazione della considerevole quantità di rischi connessi alla diffusione all'esterno di dati riservati aziendali (c.d. know-how, inteso come patrimonio cognitivo ed organizzativo, atto ad ottimizzare processi produttivi industriali), sullo smart worker incombe un onere di diligenza particolarmente qualificato (assimilabile a quello previsto ex art. 1176.2 c.c.).

A livello normativo, la tutela delle informazioni aziendali segrete (o "trade secrets", secondo il linguaggio del legislatore europeo) è affidata agli artt. 98-99 del codice della proprietà industriale, come modificati dal d. lgs. n. 63/2018, attuativo della Direttiva Ue 2016/943 ("contro l'acquisizione, l'utilizzo e la divulgazione illeciti"), nonché all'art. 2598 c.c., che in ambito civile reprime la concorrenza sleale. Detta tutela prevede anche un presidio in ambito penale: l'art. 9 del d. lgs. cit., in particolare, ha sostituito la fattispecie incriminatrice di cui all'art. 623 c.p. ("rivelazione di segreti scientifici o industriali") e punisce la condotta di chi "riveli o impieghi notizie destinate a rimanere segrete" con la reclusione fino a due anni. Ciò posto, quindi, l'obbligo comportamentale che fa capo al dipendente si snoda in un primo e più elementare dovere di evitare l'immissione in possesso dei dati aziendali da parte di un soggetto estraneo all'azienda (ad

CamminoDiritto.it
ISSN 2421-7123

esempio, un familiare convivente), come tale non autorizzato, tramite accesso ai dispositivi concessi in dotazione al lavoratore, sino a ricomprendere il dovere da parte di questi di prontamente informare il datore di lavoro in caso di sospetto (o conoscenza) del fatto che si sia verificato un accesso abusivo al sistema da parte di terzi (ovvero altra ipotesi, quale un furto, compromissione del PC, etc.).

Non da ultimo, sul lavoratore incombe anche un onere - connotato in misura significativamente qualificata - di custodire diligentemente l'elaboratore. Dal lato dell'azienda, sarebbe invece opportuna la predisposizione di sistemi di sicurezza finalizzati a consentire l'accesso ai soli file strettamente necessari per l'esecuzione della prestazione in modalità agile. In tal senso, una strategia comunemente condivisa dalle imprese è quella di accordare l'accesso alla intranet aziendale, limitandolo per l'appunto alle sole informazioni utili al lavoratore. Infine, nel novero delle più pratiche misure cautelative dei segreti commerciali, il datore di lavoro potrebbe decidere di avvalersi di modalità di accesso alle reti d'azienda, da parte degli addetti ai lavori in modalità flessibile, che si atteggino in termini di una maggiore protezione e messa al sicuro delle informazioni di cui è detentore il dipendente per conto dell'impresa nell'ambito dello svolgimento della relativa prestazione (quali, per esempio, una pendrive o un token).

Note e riferimenti bibliografici

[1] Per una più approfondita disamina, si veda A. Martone, "Smart working, job crafting, virtual team, empowerment 2018", IPSOA, 2018, pp. 67 e ss.

[2] Cfr. G. Buttarelli, "La rivoluzione copernicana del 25 maggio 2018 in materia di privacy", in Lavoro, Diritti, Europa n. 1/2018.

[3] Attuativo del decreto-legge 23 febbraio 2020, n. 6 recante "misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, applicabili sull'intero territorio nazionale"; il riferimento è, in particolare, all'art. 1 lett. n) DPCM cit. (GU Serie Generale n.55 del 04-03-2020).

[4] Più in dettaglio, a proposito delle differenti posizioni esegetiche sul punto si veda P. TULLINI, "Controlli a distanza e tutela dei dati personali del lavoratore", Torino, 2017.

[5] cfr. Garante per la protezione dei dati personali, Relazione 2016, p. 98.