SPECIALE DELLA SETTIMANA

Il controllo a distanza (non potrebbe essere altrimenti) del lavoratore in smart working: le regole d'ingaggio tra dimensione personale/familiare e dimensione lavorativa

di **Michele Palla**

L'accordo di smart working, che consente al lavoratore di prestare l'attività dedotta nel contratto di lavoro in luogo diverso da quello di pertinenza del datore di lavoro, non produce effetti particolari circa l'operatività dell'articolo 4, St. Lav., e delle regole sui controlli a distanza. È, tuttavia, evidente che per le modalità operative sue proprie, il lavoro a distanza postula una specifica informazione circa i controlli che il datore effettuerà sul lavoro del dipendente, che è opportuno inserire, da subito, nell'accordo destinato a disciplinare l'attività da remoto.

L'articolo 4, L. 300/1970, e i controlli "occulti" sul lavoratore

Il caposaldo normativo da cui prendere le mosse per l'analisi della *quaestio* del controllo a distanza del lavoratore in *smart working* è, ovviamente, rappresentato dall'articolo 4, L. 300/1970, a detta del quale, nella versione derivante dalla manutenzione del 2015 (articolo 23, D.Lgs. 151/2015), intanto, che gli impianti audiovisivi e gli "*altri strumenti*" (primi fra tutti quelli legati all'uso di pc e connessioni *internet*) dai quali derivi anche 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 previo accordo collettivo stipulato dalla Rds o dalle Rsa.

In difetto della presenza o accordo sindacale, senza stare qui a ricordare le varianti "*territoriali*" possibili, "*gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro*".

Il previo accordo sindacale o l'autorizzazione dell'Ispettorato del lavoro non sono, invece, previsti per i controlli relativi agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa[1], anche se nulla vieta, ovviamente, che il datore di lavoro pervenga comunque a un accordo di "*utilizzo*" con le OO.SS. anche in relazione a essi (ciò, a copertura di ogni successiva questione).

Per gli strumenti in questione, così come per le informazioni raccolte con gli impianti audiovisivi *et similia*, comunque, le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro, a condizione che sia data al lavoratore adeguata informazione delle

modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal c.d. Codice della *privacy*.

Anche nella nuova formulazione, dunque, l'articolo 4, St. Lav., continua a prevedere la regola per cui il controllo a distanza dell'attività dei lavoratori non è legittimo ove non sia sorretto dalle esigenze indicate dalla norma stessa. Il controllo fine a sé stesso, dunque, eventualmente diretto ad accertare inadempimenti del lavoratore che attengano all'esecuzione della prestazione dedotta in contratto, continua a essere vietato[2].

In questa prospettiva, la Suprema Corte ha più volte affermato che in nessun caso può essere giustificato un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore[3] e ciò comporta che, anche in ossequio alla normativa Europea, e segnatamente dell'articolo 8, Convenzione UE dei diritti dell'uomo, come interpretato dalla giurisprudenza della Cedu[4], occorre assicurare un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, con un contemperamento che non può prescindere dalle circostanze del caso concreto[5].

Il problema si pone, in particolar modo, per il caso dei controlli difensivi, i controlli, cioè, che il datore pone in essere per salvaguardare il patrimonio aziendale e che prescindono dalle regole dettate dall'articolo 4, St. Lav., potendo essere attuati indipendentemente dal preventivo accordo con le Rsu/Rsa (e dall'autorizzazione dell'ITL competente) e dall'informativa preventiva ai lavoratori di cui tratta l'ultimo comma della norma.

Ebbene, secondo la Corte[6], per essere in ipotesi legittimo, il controllo difensivo dovrebbe, quindi, essere mirato, nonché attuato *ex post*, ossia a seguito del comportamento illecito di uno o più lavoratori del cui avvenuto compimento il datore abbia avuto il fondato sospetto, sicché non avrebbe ad oggetto l'attività - *rectius* l'esecuzione della prestazione - ma, appunto, un'attività che da quella devia, costituendo non soltanto inadempimento, ma addirittura fatto-condotta illecito.

Anche in questo caso, però, per potersi ritenersi lecito, il controllo (difensivo) non potrebbe basarsi sull'analisi di informazioni acquisite in violazione delle prescrizioni di cui all'articolo 4, St. Lav., atteso che, in quel caso, l'area del controllo difensivo si estenderebbe a dismisura, con conseguente annientamento della valenza delle predette prescrizioni. Il datore di lavoro, infatti, potrebbe, in difetto di autorizzazione e/o di adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, nonché senza il rispetto della normativa sulla *privacy*, acquisire per lungo tempo e ininterrottamente ogni tipologia di dato riguardante l'attività del lavoratore, provvedendo alla relativa conservazione e, poi, invocare la natura mirata (*ex post*) del controllo incentrato sull'esame e analisi di quei dati.

In tal caso, secondo la Corte, il controllo non sembra potersi ritenere effettuato *ex post*, poiché esso ha inizio con la raccolta delle informazioni e quella che viene effettuata *ex post*, a quel punto, è solo un'attività successiva di lettura e analisi, che non ha, a tal fine, una sua

autonoma rilevanza: "*Può, quindi, in buona sostanza, parlarsi di controllo ex post solo ove, a seguito del fondato sospetto del datore circa la commissione di illeciti ad opera del lavoratore, il datore stesso provveda, da quel momento, alla raccolta delle informazioni*"**[7]**.

In difetto di preventiva informazione, dunque, il controllo difensivo potrebbe operare solo per il futuro, segnando il momento dell'insorgenza del sospetto (profilo, per così dire, cronologico, che starà al datore di lavoro dimostrare in giudizio in caso di contestazione della legittimità della verifica occulta), il punto di partenza delle verifiche, solo da quel momento e a quel punto legittime e lecite.

Secondo la Suprema Corte, in conclusione: "*Sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto. Non ricorrendo le condizioni suddette la verifica della utilizzabilità a fini disciplinari dei dati raccolti dal datore di lavoro andrà condotta alla stregua della L. n. 300 del 1970, art. 4, in particolare dei suoi commi 2 e 3*".

Controlli e *smart working*: l'informativa come elemento essenziale di (reciproca) tutela

Nel caso del lavoratore in *smart working*, il controllo della prestazione avverrà evidentemente sugli strumenti che egli utilizza, dovendosi peraltro considerare che, nel suo caso, la prestazione di lavoro si sgancia da una rigida predeterminazione oraria, dovendo essere valutata, per così dire, in relazione al suo risultato, per il quale il datore fisserà necessari termini di verifica.

Nell'accordo sul lavoro agile[8], dunque, dovranno essere chiariti gli obblighi del lavoratore in punto di risultati da garantire al datore nelle tempistiche date o di volta in volta comunicate, stabilendosi, ad esempio, regole specifiche circa la reperibilità/contattabilità del dipendente (per *e-mail*, sulla piattaforma digitale in uso o con altre modalità similari), nelle fasce orarie indicate.

Le fasce, ovviamente, non devono essere superiori all'orario medio giornaliero, prevendendosi una fascia minima inderogabile nella quale il lavoratore agile deve garantire la reperibilità, salve documentate esigenze, magari prevedendosi da subito che l'impossibilità di contattare il lavoratore nelle fasce concordate può portare alla risoluzione dell'accordo di *smart working* (salve improvvise e comprovate ragioni tecniche o personali di natura contingente che giustifichino la "latitanza" del dipendente).

Nell'accordo poi, al lavoratore in modalità agile dev'essere garantito:

a) il rispetto della fascia di inattività, coincidente con il periodo di tempo in cui non può essere erogata alcuna prestazione lavorativa nel rispetto delle previsioni del D.Lgs. 66/2003 (si pensi all'articolo 7 e al periodo di 11 ore di riposo consecutivo);

b) l'esercizio del diritto alla disconnessione, da intendersi come diritto del lavoratore a disconnettersi dalle strumentazioni tecnologiche e dalle piattaforme informatiche utilizzate per svolgere la prestazione lavorativa e in virtù del quale non sono richiesti contatti con i colleghi o con i superiori per lo svolgimento della prestazione lavorativa, la lettura delle *e-mail*, l'accesso e la connessione al sistema informativo del datore[9].

Ciò detto in via di davvero estrema sintesi sulle regole basilari del lavoro agile, è certo che anche in relazione al lavoro a distanza valgono, nella loro integrità, le prescrizioni dell'articolo 4, St. Lav., sopra riportate. In questa prospettiva, e per presidiare la riservatezza del lavoratore mediandola con i possibili controlli del datore, è opportuno che, sin dalla stesura dell'accordo di *smart working*, il datore espliciti per iscritto le eventualità modalità di effettuazione del controllo, la tipologia di informazioni che potranno essere acquisite e, infine, la modalità di trattamento, gestione e conservazione delle informazioni e dati così ottenuti.

In questo modo, viene rispettata la condizione dell'articolo 4, comma 3, L. 300/1970, che, come detto, condiziona l'utilizzo dei dati acquisiti all'adeguata, dovuta informazione al lavoratore delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal c.d. Codice della *privacy*. Ovviamente, le regole che vietano il controllo anelastico e permanente della prestazione (articoli 2, 3 e 4, St. Lav.) inibiscono al datore la possibilità di modificare lo strumento di lavoro assegnato al lavoratore agile, ad esempio il *pc*, per consentire verifiche occulte, magari installando su di esso, prima della consegna, *software* di localizzazione o che in qualunque modo monitorino il lavoro a distanza del dipendente[10].

Nel caso in cui il lavoratore in *smart working* utilizzi *internet* o sia assegnatario di una casella di posta elettronica, poi, il controllo del datore di lavoro potrà essere effettuato avendo ben presenti le linee guida emanate dal Garante *privacy* (in attuazione, verrebbe da dire, delle disposizioni dello Statuto dei lavoratori) con la delibera n. 13/2007.

Secondo il Garante, ad esempio, è legittima la raccolta di dati con *proxy server* o altri strumenti, a patto che ciò riguardi la tutela di beni estranei al rapporto di lavoro (come il patrimonio aziendale) e non la verifica sull'adempimento della prestazione lavorativa. In queste ipotesi l'azienda è comunque tenuta a informare i dipendenti:

1. sul corretto utilizzo della linea *internet*;
2. sulle modalità di svolgimento dei controlli; sui comportamenti non concessi rispetto alla navigazione *internet* (ad esempio, il *download* di *file* musicali);
3. sui limiti di utilizzo della linea *internet* per scopi personali, come l'uso circoscritto alle pause intermedie;
4. sulle conseguenze di tipo disciplinare per le condotte contrarie ai limiti prescritti.

È ovvio che tutte queste regole debbono essere armonizzate con la specifica realtà del lavoro in *smart working*, specie laddove - ed è *modus operandi* che di fatto non è eccezionale - il dipendente utilizzi il suo *pc* e magari la sua connessione privata, anche se il datore di lavoro in qualche modo indennizzi l'uno e l'altra, atteso che, in quel caso, l'integrazione di dimensione personale/familiare e dimensione lavorativa rischia di essere inestricabile: a maggior ragione, occorre che nell'accordo di *smart working* vengano specificate le regole operative del lavoro a distanza e quelle relative al controllo del datore di lavoro, con specifico riferimento alle condotte che il lavoratore agile non deve tenere.

In particolare, sarà opportuno esplicitare ancor meglio, rispetto a quanto comunemente fatto con i lavoratori che operano nei locali del datore, le modalità d'uso della casella di posta elettronica aziendale e degli eventuali programmi, anche di navigazione, che il datore metta a disposizione del dipendente per lavorare a distanza.

Quanto, poi, ai controlli difensivi, valgono tal quali le regole già evidenziate sul piano generale: in caso di fondato sospetto di condotte illecite dello *smart worker*, di conseguenza, il datore potrà attivare i controlli difensivi, avendo cura di rispettare le regole che già sono state ricordate *supra*.

Conclusioni

L'accordo di *smart working* che consente al lavoratore di prestare l'attività dedotta nel contratto di lavoro in luogo diverso da quello/quelli di pertinenza del datore di lavoro non produce effetti particolari circa la (piena) operatività dell'articolo 4, St. Lav., e la operatività delle regole sui controlli a distanza.

È, tuttavia, evidente che, per le modalità operative sue proprie, il lavoro a distanza o agile che dir si voglia, postula una specifica informazione circa i controlli che il datore effettuerà sul lavoro del dipendente, che è opportuno inserire, da subito, nell'accordo destinato a disciplinare l'attività da remoto: in quel modo, il datore di lavoro potrà, all'occorrenza, fornire prova documentale dell'informativa postulata dall'articolo 4, comma 3, L. 300/1970.

Il controllo non potrà che modellarsi sugli impegni e sulle regole che governano e caratterizzano il lavoro a distanza, risultando comunque opportuna, o sarebbe meglio dire indispensabile, una specifica delimitazione degli impegni del lavoratore agile, così da ritagliare un perimetro comunque identificabile a contorno di una vicenda professionale che, inevitabilmente, presenta commistioni con la vita personale e familiare del lavoratore.

[1] E agli strumenti di registrazione degli accessi e delle presenze.

[2] Per dar vita a una sinergia circa il controllo degli abusi dei controlli a distanza si veda il protocollo sottoscritto il 22 aprile 2021 tra l'INL e il Garante per la protezione dei dati personali.

[3] Cassazione, n. 16622/2012, in Riv. giur. lav., 2013, II, 32 (m), n. Mettei e Lav. giur., 2013, 383, n. Barraco, Sitzia; Cassazione n. 9904/2016, in Lavoro e prev. oggi, 2016, 724, n. Viceconte; Cassazione n. 18302/2016, in Riv. it. dir. lav., 2017, II, 26, n. Criscuolo, Ingrao.

[4] Corte Europea dei diritti dell'uomo. Nel caso Barbulescu c. Romania, sentenza della Grande Camera del 5 settembre 2017, la Corte Europea dei diritti dell'uomo, chiamata a pronunciarsi - in relazione al detto articolo 8, Convenzione UE dei diritti dell'uomo - con riguardo a una vicenda in cui un datore di lavoro aveva sottoposto a controllo il *software* aziendale *Yahoo Messenger* in uso al lavoratore, onde verificarne un indebito utilizzo, ha fornito un'interpretazione estensiva del concetto di "*vita privata*", tanto da includervi la "*vita professionale*", così ritenendo che lo Stato rumeno avesse tenuto un comportamento non conforme alle garanzie accordate dalla norma della Convenzione, per avere le Corti nazionali omesso di accertare se il lavoratore avesse ricevuto una preventiva informazione dal suo datore di lavoro della possibilità che le sue comunicazioni su *Yahoo Messenger* potessero essere controllate; inoltre, per non avere valutato se il lavoratore medesimo fosse stato posto a conoscenza della natura e dell'estensione del controllo o del grado di intrusione nella vita e nella corrispondenza privata; infine, per non avere accertato le specifiche ragioni che giustificavano l'adozione di dette misure di controllo e se il datore di lavoro avrebbe potuto utilizzare misure meno intrusive, ne se l'accesso al contenuto delle comunicazioni fosse stato compiuto senza che il lavoratore ne avesse consapevolezza.

[5] Cassazione, n. 26682/2017, in Lav. giur., 2018, 471, n. Levi.

[6] Cassazione, n. 25732/2021. In termini e sulla prova del "*fondato, legittimo sospetto*" all'origine del controllo difensiva, si veda Cassazione, n. 18168/2023.

[7] In via esemplificativa, la Corte richiama il classico esempio dei dati di traffico contenuti nel *browser* del *pc* in uso al dipendente, stabilendo: "*potrà parlarsi di controllo ex post solo in relazione a quelli raccolti dopo l'insorgenza del sospetto di avvenuta commissione di illeciti ad opera del dipendente, non in relazione a quelli già registrati*".

[8] In relazione ai requisiti e ai contenuti dell'accordo individuale di *smart working*, si veda l'accordo tra Mlps e OO.SS. del 7 dicembre 2021 sul primo "*Protocollo Nazionale sul lavoro in modalità agile nel settore privato*". Con il D.M. 149/2022 - e relativi Allegati - sono state definite le modalità per assolvere agli obblighi di comunicazione previsti dall'articolo 23, comma 1, L. 81/2017 (come modificato dall'articolo 41-*bis,* D.L. 73/2022, convertito con modificazioni in L. 122/2022) e, quindi, per inviare telematicamente le informazioni relative all'accordo di lavoro agile. Infatti, in base alla nuova disciplina non è più necessario allegare l'accordo individuale di *smart working* sottoscritto tra datore di lavoro e lavoratore (che deve essere comunque conservato dal datore di lavoro ai fini della prova e della regolarità amministrativa per 5 anni

dalla sottoscrizione), ma trasmettere al Ministero le informazioni individuate nel Decreto stesso e negli Allegati che ne formano parte integrante.

[9] Nel protocollo nazionale sul lavoro agile (vedi nota che precede) è stabilito quanto segue. Articolo 3: "*1. Ferme restando le previsioni di legge e di contratto collettivo, la giornata lavorativa svolta in modalità agile si caratterizza per l'assenza di un preciso orario di lavoro e per l'autonomia nello svolgimento della prestazione nell'ambito degli obiettivi prefissati, nonché nel rispetto dell'organizzazione delle attività assegnate dal responsabile a garanzia dell'operatività dell'azienda e dell'interconnessione tra le varie funzioni aziendali. 2. La prestazione di lavoro in modalità agile può essere articolata in fasce orarie, individuando, in ogni caso, in attuazione di quanto previsto dalle disposizioni normative vigenti, la fascia di disconnessione nella quale il lavoratore non eroga la prestazione lavorativa. Vanno adottate specifiche misure tecniche e/o organizzative per garantire la fascia di disconnessione. 3. Il lavoratore può richiedere, ove ne ricorrano i relativi presupposti, la fruizione dei permessi orari previsti dai contratti collettivi o dalle norme di legge quali, a titolo esemplificativo, i permessi per particolari motivi personali o familiari, di cui all'art. 33 della legge 5 febbraio 1992, n. 104. 4. Salvo esplicita previsione dei contratti collettivi nazionali, territoriali e/o aziendali, durante le giornate in cui la prestazione lavorativa viene svolta in modalità agile non possono essere di norma previste e autorizzate prestazioni di lavoro straordinario. 5. Nei casi di assenze c.d. legittime (es. malattia, infortuni, permessi retribuiti, ferie, ecc.), il lavoratore può disattivare i propri dispositivi di connessione e, in caso di ricezione di comunicazioni aziendali, non 4 è comunque obbligato a prenderle in carico prima della prevista ripresa dell'attività lavorativa. 6. Compatibilmente con l'organizzazione aziendale, le esigenze produttive e l'attività svolta dal lavoratore, al lavoro agile possono accedere, previo accordo individuale ex art. 19, l. n. 81/2017, i lavoratori inseriti nelle aree organizzative in cui lo stesso viene utilizzato".*

[10] Il Garante *privacy*, nelle Linee guida del 2007 (si veda *infra*), ha precisato che nell'esercizio del potere di controllo occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "*apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori*" (articolo 4, comma 1, L. 300/1970), tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente di un sistema di comunicazione elettronica. Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli: "*In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire –a volte anche minuziosamente– l'attività di lavoratori".*

Si segnala che l'articolo è tratto da "**Il giurista del lavoro**".