derecom

ISSN: 1988-2629. Nº. 29. Nueva Época. Septiembre 2020-Marzo 2021

Cómo citar este texto:
Furios, Ch. (2020). Controllo dei lavoratori in smart working. *Derecom*, 29, 57-74, http://www.derecom.com/derecom/

CONTROLLO DEI LAVORATORI IN SMART WORKING

CONTROL DE LOS TRABAJADORES EN RÉGIMEN DE TELETRABAJO

CONTROL OF WORKERS DURING SMART WORKING

© Chiara Furios
Instituto Nacional Italiano de la Seguridad Social
cfurios@ucm.es

Riassunto

L'articolo vuole evidenziare come le nuove tecnologie offrano modalità indirette di controllo del lavoratore.

Come sappiamo, lo Statuto dei Lavoratori regola le modalità con cui il datore di lavoro può controllare il lavoratore, ponendogli una serie di limiti, ad esempio nell'installazione di telecamere, nelle modalità di rilevamento della presenza, nel controllo della navigazione tramite Internet e uso della posta elettronica.

L'emergenza COVID-19 ha incrementato in modo improvviso e senza precedenti la percentuale di lavoratori in smart working e quindi le forme di controllo sul lavoratore sono necessariamente cambiate rispetto a quelle applicate all'interno della sede aziendale.

Per la tutela della dignità, della privacy e della libertà di comunicazione è necessario aggiornare le forme di tutela e informazione del lavoratore.

L'articolo illustrerà come sia possibile controllare il telelavoratore attraverso il controllo delle sessioni, la posta elettronica e come l'utilizzo dei computer e dello smartphone dell'azienda permetta al datore di lavoro di monitorare ogni attività che ha avuto luogo, anche durante l'orario non lavorativo, in questi dispositivi.

Resumen

El artículo tiene como objetivo destacar cómo las nuevas tecnologías ofrecen formas indirectas de controlar al trabajador.

Recibido: 21/08/2020 Revisado: 03/09/2019
Aceptado: 08/09/2020 Publicado:15/09/2020

Como sabemos, el Estatuto de los Trabajadores regula las formas en que el empleador puede controlar al trabajador, poniéndole una serie de límites, por ejemplo en la instalación de cámaras, en las modalidades de detección de presencia, en el control de navegación y uso de Internet. correo electrónico.

La emergencia COVID-19 ha incrementado repentina y sin precedentes el porcentaje de trabajadores en el trabajo inteligente y por tanto las formas de control sobre el trabajador han cambiado necesariamente respecto a las aplicadas dentro de la sede de la empresa.

Para la protección de la dignidad, la intimidad y la libertad de comunicación es necesario actualizar las formas de protección e información del trabajador.

El artículo ilustrará cómo es posible controlar al teletrabajador a través del control de sesión, el correo electrónico y cómo el uso de las computadoras y el teléfono inteligente de la empresa permite al empleador monitorear cada actividad que ha tenido lugar, incluso durante la horario no comercial, en estos dispositivos.

Summary

In the paper we highlight the multitude of controls that employers can implement against workers who carry out their teleworking tasks, through "indirect" methods made available by new technologies.

As we know, the italian Statuto dei Lavoratori regulates the ways in which the employer can control its employee, imposing a series of limits, for example, in the installation of cameras, in the methods of detection of presence, in the control of navigation by internet and email.

The COVID-19 emergency has suddenly and unprecedentedly increased the number of teleworkers and then the forms of monitoring over the workers have necessarily changed compared to those applied within the company headquarters.

Thanks to new technologies, it is now possible to use extremely sophisticated remote monitoring systems towards workers.

For the protection of dignity, privacy and freedom of communication, it is necessary to update the forms of protection and information of the workers.

The article will illustrate how it is possible to control the teleworker through session control, email and how using the company's computers and smartphones makes it possible for the employer to monitor each activity that has taken place, also during non-working hours, in these devices.

Parole chiave: Smart working. Telelavoro. Lavoro agile. Controllo dei lavoratori

Palabras clave: Smart working. Teletrabajo. Trabajo ágil. Control de trabajadores

Key words: Smart working.Telework. Agile work. Control of workers

1. Introduzione: contesto

La tematica del controllo sui lavoratori è stata molto dibattuta a livello giurisprudenziale e dottrinale. Su questo argomento si confrontano due contrapposti interessi: da un lato quello del datore di lavoro che vuole tutelare la produttività, i beni aziendali e assicurarsi nel contempo che i dipendenti svolgano con diligenza l'attività per cui sono pagati, dall'altro quello dei lavoratori che desiderano difendere la propria privacy ed evitare che i controlli aziendali sul lavoro siano troppo invasi, lesivi della riservatezza e della dignità personale.

In ambito giuridico, ogniqualvolta interessi contrapposti si fronteggiano è necessario attuare un bilanciamento tra le finalità perseguite dalle due parti. Nel caso specifico del controllo sull'attività del lavoratore, le due esigenze da ponderare, entrambe leggittime, sono da una parte quella del datore di lavoro che ha la necessità di tenere sotto controllo la produttività e proteggere il patrimonio aziendale e la sicurezza dei lavoratori, e dall'altra il lavoratore che vuole che siano garantite la propria dignità, il diritto alla riservatezza nelle comunicazioni, la libertà di movimento.

Affinché i controlli della parte datoriale possano essere compatibili con le esigenze di privacy dei lavoratori, essi devono essere strettamente disciplinati, al fine di evitare abusi da un lato, e dall'altro consentire un livello di controllo che risulti di una qualche efficacia ai fini della salvaguardia della produttività.

2.Il controllo nello Statuto dei Lavoratori

Un primo tentativo di bilanciare detti opposti interessi si ebbe con la stesura dello Statuto dei Lavoratori nel 1970 (legge n. 300 del 1970), quando si era ancora ben lungi dal considerare la privacy come un diritto costituzionalmente garantito.[1] Lo Statuto dei Lavoratori, nel titolo I, tutela la libertà e la dignità del lavoratore, salvaguardando la sua libertà di opinione, vietando indagini sulle sue opinioni, tutelando il diritto all'istruzione dei lavoratori-studenti, promuovendo le attività culturali, ricreative e assistenziali, tutelando la salute ed evitando accertamenti sanitari e visite personali arbitrarie e, per quanto concerne l'argomento in esame, vietando l'utilizzo di strumenti che permettono il controllo a distanza dei lavoratori.[2]

Nello specifico, lo Statuto dei Lavoratori nell'art. 2 dispone che l'attività di vigilanza delle guardie giurate si limiti esclusivamente alla difesa del patrimonio aziendale, tanto da vietarne l'accesso ai luoghi di lavoro e precludendo loro qualsiasi possibilità di contestazione sull'operato dei lavoratori che non riguardi un ammanco di beni aziendali.

Nella sua formulazione originaria, lo Statuto dei Lavoratori vietava il controllo dell'attività dei lavoratori sia attraverso l'impiego di guardie giurate sia a distanza, ovvero, come recitava il comma 1 dell'art. 4, attraverso l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. L'art. 4 è tuttavia stato modificato nel 2015,[3] eliminando il primo comma, che vietava in via generale l'uso di apparecchiature per finalità di controllo a distanza dei lavoratori[4] e lo rendeva possibile solo in casi eccezionali.[5] La riforma ha introdotto la possibilità di utilizzare strumentazione atta a un controllo a distanza

dell'attività dei lavoratori purché connessa ad esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale, previo accordo con le rappresentanze sindacali o, in loro mancanza, con un'autorizzazione dell'Ispettorato del lavoro, che dovrà precisare modalità e adeguamenti dei controlli al fine di garantire la privacy del lavoratore.

È impossibile non notare la riforma del 2015 comporti un notevole ampliamento delle possibilità di controllo datoriale dovuto all'eliminazione del divieto generale di controllo a distanza e alla facilità con cui è possibile ricondurre qualsiasi forma di controllo del lavoratore all'interno delle fattispecie previste dalla norma. È importante sottolineare che la riforma ha introdotto tra le esigenze di controllo dell'attività dei lavoratori la tutela del patrimonio aziendale, in cui è possibile far rientrare tutto ciò che comporta un costo per l'azienda. Sebbene, dunque, la riforma consenta esclusivamente un controllo "incidentale" sull'attività del lavoratore, ovvero un controllo indiretto in quanto non mirato al controllo del lavoratore bensì alla difesa del patrimonio aziendale o di specifiche esigenze organizzative e produttive, permette di fatto un controllo sul lavoratore. Negli ultimi anni, dunque, la situazione del lavoratore risulta notevolmente peggiorata per essenzialmente due cause: la prima scaturisce dall'ampliamento dei controlli datoriali concessa dal legislatore e la seconda dalla nascita di nuove tecnologie che permettorno un controllo sull'attività e sul lavoratore inimmaginabili nel 1970. Inoltre, se gli strumenti di controllo a distanza avevano un costo notevole negli anni '70, oggi strumenti di controllo, anche molto invasivi, sono alla portata anche del più piccolo imprenditore.

Non si deve pensare che prima della riforma fosse preclusa al datore di lavoro qualsiasi forma di controllo sull'attività lavorativa. Al datore di lavoro è sempre consentito effettuare controlli diretti, ovvero non a distanza, sull'operato dei propri dipendenti. Può farlo direttamente o tramite propri delegati che non siano, come disciplinato dall'art. 2 dello Statuto dei Lavoratori, guardie giurate. Tali controlli possono effettuarsi anche di nascosto, purché siano "analogici", effettuati ad esempio tramite il datore di lavoro che osserva il lavoratore, e non in modo tecnologico, cioè utilizzando telecamere *et similia.*[6]

3.La tutela della "privacy" del lavoratore (GDPR)

Il controllo sull'operato dei lavoratori, oltre ai vincoli e alle possibilità delineati dalla Costituzione e dallo Statuto dei Lavoratori, deve sottostare ai limiti imposti dalla legislazione a tutela della privacy degli individui, che negli stati membri dell'Unione Europea è rappresentata dal regolamento UE 2016/679 (cosiddetto GDPR) che ha modificato la normativa nazionale preesistente, disciplinata dal D. Lgs. 196/2003 (cosiddetto Codice della Privacy). Il GDPR ha infatti, tra l'altro, dato attuazione all'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea che tutela il diritto alla protezione dei dati personali facendolo rientrare tra i diritti fondamentali dell'individuo,[7] disciplinando il trattamento dei dati personali delle persone fisiche.

Il GDPR individua processi, ruoli e responsabilità per la gestione, la conservazione e l'esportazione dei dati personali dei cittadini europei o di cittadini residenti in Unione Europea. Dal punto di vista dei ruoli, particolare importanza assumono il Titolare e il Responsabile del trattamento dei dati. Il primo è colui che stabilisce le modalità e le finalità del trattamento dei dati; il secondo è colui che tratta i dati personali per conto del Titolare e può essere anche un soggetto estero rispetto all'unità organizzativa del Titolare. Per quanto riguarda i processi da mettere in atto, secondo il GDPR, per la protezione e tutela dei dati personali, riveste particolare importanza nell'ambito dei controlli a distanza sul lavoratore la Valutazione d'impatto, o DPIA.

4.Valutazione d,impatto (Data Protection Impact Assessment)

La valutazione d'impatto, conosciuta con l'acronimo DPIA, è una procedura regolata dall'art 35 GDPR[8] che mira a valutare quanto un'attività posta in essere dal datore di lavoro per tutelare i propri interessi risulti compatibile, necessaria, proporzionata e quali rischi comporti alla privacy del dipendente; dove per privacy del dipendente intendiamo in questo caso il diritto alla riservatezza, alla libertà negli spostamenti, alle tutele previste dallo Statuto dei lavoratori.[9] La valutazione d'impatto deve essere effettuata ogniqualvolta un trattamento dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori). Il GDPR impone a colui che è responsabile dell'ottemperanza degli obblighi previsti dalla normativa sulla privacy di intraprendere una valutazione di impatto prima di dare inizio a una qualsiasi delle attività elencate dall'art. 29 GDPR.[10] In tali attività rientrano: l'accesso ai dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza; l'acquisizione di dati relativi alla geolocalizzazione di un dispositivo dal quale si possa dedurre il luogo in cui si trova il dipendente, poiché questo incide sull'esercizio di un diritto fondamentale della persona, ossia la libertà di movimento; l'utilizzo di sistemi di videosorveglianza dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti.

5.I controlli a distanza

Una prima distinzione, dunque, che emerge nell'ambito dei controlli sul lavoratore è quella tra controlli in presenza e controlli a distanza. I controlli in presenza sono eseguiti in prima persona dal datore di lavoro o da un suo delegato tramite l'osservazione diretta dei lavoratori nel proprio ambiente di lavoro. Per controllo a distanza si intende tutto ciò che non rientra nella prima categoria, e cioè qualsiasi modalità che consente al datore di lavoro di controllare l'attività del lavoratore senza essere fisicamente presente. Rientrano dunque nei controlli a distanza la sorveglianza tramite videocamere, l'accesso alla cronologia della navigazione in Internet dal PC dell'ufficio o al registro delle telefonate effettuate e ricevute dal telefono dell'ufficio.

Fino a questo punto abbiamo visto le modalità e i limiti del controllo del lavoratore all'interno del posto di lavoro e tutto sommato possiamo dire che la difesa della privacy del lavoratore è garantita all'interno della sede aziendale, sia essa fabbrica oppure ufficio, ma tutto risulta più sfumato, di più difficile definizione quando il lavoratore lavora da casa in smart working.[11] La privacy del lavoratore in smart working è più vulnerabile poiché la normativa ancora non è aggiornata con le varie modalità di controllo che si possono operare utilizzando i sistemi informatici.

6.Lavoro in "smart working" con uso di strumentazione personale

Quando il lavoratore in smart working usa strumentazione propria, cioè personal computer, telefono cellulare, SIM, connessione a Internet, etc. di sua proprietà, non forniti, quindi, in dotazione dall'azienda, ci troviamo di fronte a una fattispecie particolare di smart working, chiamata "lavoro agile semplificato" e introdotta dall'art. 87 del D.L. 18/2020, convertito dalla L. 27/2020.

Nella concezione tradizionale del lavoro data dalla teoria economica, l'imprenditore fornisce il lavoro e i mezzi produttivi e il lavoratore la propria opera; tale concezione è mantenuta anche nell'impianto originario che regola lo smart working, che nel testo normativo viene chiamato "lavoro agile". La L. 81/2017, che al capo II disciplina il lavoro agile, dispone testualmente all'articolo 18, secondo comma, che: *Il datore di lavoro è responsabile della sicurezza e del buon funzionamento degli strumenti tecnologici assegnati al lavoratore per lo svolgimento dell'attivita' lavorativa*. Ciò significa che nella volontà del legislatore, ad esempio, il personal computer con il quale svolgere il lavoro agile è fornito dall'azienda, e in caso di guasto o caduta accidentale, l'intervento di un tecnico specializzato per la riparazione o la sostituzione dell'apparecchio è a carico del datore di lavoro.

Nello smart working operato con strumentazione personale, invece, anche i mezzi produttivi sono di proprietà del lavoratore, limitandosi di fatto l'imprenditore a fornire il lavoro da svolgere, che si tratti di pratiche da evadere, bilanci da redigere o progetti da condurre.

La stessa L. 81/2017 impone che lo smart working sia subordinato alla sottoscrizione da ambo le parti di uno specifico accordo, nel quale, tra le altre cose, devono essere specificate eventuali forme di controllo a distanza che il datore di lavoro potrà intraprendere, nonché i comportamenti del lavoratore che possono condurre a sanzioni disciplinari.[12] La modifica emergenziale introdotta dal D.L. 18/2020 ha derogato anche a questo aspetto, e pertanto per quanto inerente i controlli a distanza del lavoratore in smart working si applica la normativa generale prevista dall'art. 4 dello Statuto dei Lavoratori.

7.Lavoro in "smart working" con uso di strumentazione aziendale

L'utilizzo di strumentazione aziendale per il lavoro agile rende possibile l'adozione di misure di controllo a distanza dell'attività del lavoratore più invasive rispetto all'uso di strumenti personali del dipendente. Questo perché gli strumenti di lavoro non rientrano tra i dispositivi di controllo a distanza disciplinati dall'art. 4 dello Statuto dei Lavoratori, ma al contempo rendono possibili attività di controllo, persino intriseche all'utilizzo dello strumento. Ad esempio, il datore di lavoro può avere la possibilità di esaminare la cronologia di navigazione in Internet dei browser installati sui computer aziendali, e nel caso rilevi un uso improprio del computer aziendale o si documenti che il lavoratore ha perseguito finalità estranee all'attività lavorativa durante l'orario di lavoro, il dipendente potrebbe incorrere in sanzioni disciplinari.

Anche in questo caso vi è una differenza sostanziale tra il lavoro agile ex L. 81/2017 e il lavoro agile semplificato. Nel primo caso la normativa sullo *smart working* prevede che le eventuali forme di controllo che la parte datoriale potrà esercitare debbano essere esplicitate nell'accordo di lavoro agile sottoscritto individualmente tra datore di lavoro e lavoratore. Nel caso di smart working semplificato, poiché non vi è alcun accordo sottoscritto che ne regoli lo svolgimento, quando il lavoratore utilizza strumenti forniti in dotazione dall'azienda si applicano le stesse medesime regole del lavoratore che svolge la sua attività presso le sedi aziendali, per cui, non essendo tali dispositivi considerati alla stregua degli impianti audiovisivi e altri strumenti di controllo ex art. 4 L. 300/1970, bensì strumenti di lavoro, l'attività di controllo esplicata indirettamente tramite essi non è sottoposta ad alcun accordo sindacale né all'autorizzazione dell'Ispettorato del Lavoro.

Questo non significa che l'azienda possa usare il cellulare o il computer dato in dotazione al dipendente per controllarlo, ma può farlo in modo indiretto. Se, ad esempio, il dipendente usa tale strumentazione di proprietà aziendale per scopi personali durante l'orario di lavoro, l'azienda per tutelare il proprio patrimonio e la produttività o per esigenze organizzative, può

verificare l'uso improprio del dispositivo attraverso i registri delle chiamate o la cronologia della navigazione in Internet e, nel caso, applicare una sanzione disciplinare.

Per forza di cose, effettuando questo genere di controlli, il datore di lavoro ha modo di monitorare anche l'attività extralavorativa del proprio dipendente. Sebbene tali informazioni non abbiano alcuna rilevanza all'interno del rapporto di lavoro, a meno che non comportino un danno all'azienda, è innegabile che esse consentano al datore di lavoro di venire a conoscenza, ad esempio, dei destinatari delle chiamate e delle abitudini di navigazione del dipendente, e questo configura un'invasione della privacy.

Ipotizziamo che un dipendente usi per scopi extra-lavorativi il cellulare aziendale effettuando chiamate verso un numero a pagamento. In questo caso, sia che ciò avvenga durante l'orario di lavoro sia fuori, qualora il lavoratore sia stato precedentemente informato sulla possibilità e modalità del controllo sulle chiamate, l'acquisizione delle informazioni si sia limitato a quanto strettamente necessario, senza ledere la privacy e la dignità del lavoratore, e da tale controllo risultasse un danno economico al patrimonio aziendale, sussisterebbe la possibilità per il datore di lavoro di richiedere al lavoratore il rimborso del danno economico causato o, in determinati casi,[13] di intraprendere un procedimento disciplinare[14] nei confronti del lavoratore.

La sanzione disciplinare potrà essere applicata solo in presenza di alcuni presupposti:[15] che il controllo sull'uso della strumentazione per scopi extra-lavorativi comporti un danno economico all'azienda e che il lavoratore sia stato informato su detti controlli. Il lavoratore dovrà essere reso edotto, in modo dettagliato, sull'ampiezza dei controlli, sulle loro modalità e deve aver firmato per presa visione un protocollo dal quale deve risultare in maniera chiara ciò che è consentito fare e ciò che invece è proibito fare con i beni aziendali. I dati sulle chiamate devono essere conservati per un tempo massimo di sei mesi. Il controllo deve limitarsi a quanto strettamente necessario.

Indubbiamente, si è riusciti a far accettare di buon grado ai lavoratori questa notevole interferenza nella loro sfera privata facendo passare la dotazione di strumenti tecnologici (cellulare, personal computer e tablet aziendali) come benefit aziendali.

8.Strumenti di lavoro che consentono un controllo indiretto sull´attività del lavoratore

In modo analogo a quanto avviene per il controllo su cellulari e personal computer, è possibile un controllo da parte del datore di lavoro sulla casella di posta elettronica aziendale[16] solo in casi eccezionali.[17]

8.1 Email

La posta elettronica è una forma di comunicazione che può essere equiparata alla corrispondenza tradizionale e la cui riservatezza e segretezza riceve a livello costituzionale apposita tutela.[18]

Al fine di evitare inopportune ingerenze nella sfera privata del dipendente, risulteranno efficaci alcune misure da attuare al fine di permettere l'accesso alle comunicazioni anche in assenza del lavoratore, ad esempio predisponendo email comuni a cui tutti i dipendenti di un certo ufficio possono accedere (ad esempio ufficiosinistri@nomeditta.com) oppure predisporre

una risposta automatica nell'email del dipendente che informi l'interlocutore dei vari nominativi a cui rivolgersi durante la sua assenza. Tutto questo permette all'azienda di continuare a svolgere la propria attività senza dover accedere alla casella email del dipendente.

Anche il controllo della casella email deve essere finalizzato esclusivamente alla protezione del patrimonio aziendale, a esigenze organizzative e produttive, oppure per garantire la sicurezza del lavoro. Nel patrimonio aziendale, che come si è sottolineato in precedenza è stato oggetto di recente introduzione tra le finalità dei controlli, è possibile far rientrare anche l'orario di lavoro, durante il quale il lavoratore dovrebbe dedicarsi esclusivamente a svolgere l'attività per cui è stato assunto e viene pagato. Il controllo della casella di posta elettronica rimane possibile purché il lavoratore sia stato reso edotto sui possibili controlli, questi ultimi si limitino a quanto strettamente necessario a tutelare gli interessi del datore di lavoro, in quanto la dignità e privacy del lavoratore devono sempre essere opportunamente protette. Nel caso in cui sia sollevata una contestazione nei confronti del lavoratore, il datore di lavoro dovrà dichiarare quali e quante email sono state osservate, in che lasso di tempo e i nominativi delle persone che hanno effettuato l'accesso ai fini del controllo.

8.2 Geolocalizzazione del lavoratore

I sistemi GPS (Global Positioning System) permettono di conoscere l'esatta ubicazione di un veicolo aziendale oppure di un tablet, smartphone[19] o personal computer.

Questi sistemi di geolocalizzazione sono strumenti aggiuntivi rispetto agli strumenti di lavoro veri e propri. Se si prendono in considerazione, ad esempio, i furgoni portavalori, lo strumento di lavoro è rappresentato dal veicolo necessario a effettuare il trasporto del denaro; la presenza sul veicolo di un rilevatore satellitare che consente alla centrale operativa di seguire in tempo reale gli spostamenti del mezzo, giustificato da esisgenze di tutela dei valori trasportati, consente però in modo indiretto anche il controllo dei lavoratori presenti sul mezzo. Pertanto, per l'installazione del trasponder satellitare risulterà necessario l'accordo con le rappresentanze sindacali o l'autorizzazione dell'Ispettorato del Lavoro[20] e, naturalmente, i lavoratori dovranno essere portati a conoscenza della presenza di tale dispositivo.

Come detto, simili dispositivi possono essere attivati anche su smartphone e personal computer, e in questi casi oltre all'accordo dei sindacati o all'autorizzazione dell'Ispettorato del Lavoro[21] sui display deve apparire un'icona che indichi quando la funzionalità di geolocalizzazione risulta attiva. Inoltre, deve essere data la possibilità di disattivare la funzione durante le pause lavorative previste dalla legge.[22] Di tutto ciò i lavoratori devono essere debitamente informati e risulterà opportuno dotare il dispositivo di un sistema di oscuramento del GPS decorso un dato periodo di inattività.

8.3 Rilevazione della presenza attraverso laconnessione alle risorse aziendali

Quando il lavoro si svolge da remoto, non è fisicamente possibile verificare la presenza del lavoratore e il rispetto dell'orario lavorativo, poiché il lavoratore stesso non ha possibilità di azionare i tradizionali sistemi di marcatura di ingressi e uscite installati presso la sede di lavoro. Poiché però, nella maggior parte dei casi, il lavoratore ha necessità, per lo svolgimento dei propri compiti lavorativi, di connettersi a risorse aziendali, quali banche dati, software proprietari, intranet aziendale, email aziendale, VPN, cartelle condivise, etc. e tali accessi sono automaticamente registrati dai sistemi informatici che li erogano, il datore di lavoro ha la possibilità, accedendo a tali registri, di verificare orari di connessione e disconnessione e durata della sessione di lavoro.

Per quanto attiene a questo genere di controlli, non è prevista alcuna specifica informativa al lavoratore, né è richiesta un'apposita accordo sindacale o autorizzazione dell'Ispettorato del Lavoro, poiché essi sono connaturati all'utilizzo degli strumenti sopra descritti.

8.4 Strumenti di web analytics applicati alle risorse web aziendali

All'interno delle aziende il web costituisce ormai il mezzo privilegiato per la diffusione di informazioni e risorse, come news aziendali, normative, circolari, ordini di servizio, indispensabili per la formazione continua e l'aggiornamento dei dipendenti, che vengono pubblicate sulla intranet aziendale e spesso condivise con i dipendenti tramite newsletter interne. Al fine di migliorare le modalità comunicative che un'azienda, soprattutto se di grosse dimensioni, deve costantemente tenere aggiornate al fine di incrementare la professionalità e il *commitment* dei dipendenti, le aziende utilizzano strumenti di *web analytics*, *tool* che permettono di raccogliere, misurare e comparare i dati di utilizzo dei siti web originariamente nati per l'utilizzo su Internet, per misurare l'efficacia del *medium* utilizzato per comunicare con i lavoratori. Ad esempio, il datore di lavoro potrebbe rendersi conto che una novità normativa da portare a conoscenza dei dipendenti, se comunicata tramite email viene letta da un numero limitato di dipendenti, mentre se la stessa notizia è pubblicata con un grande riquadro nell'*home page* della intranet viene visualizzata da tutti. I web analytics, dunque, hanno lo scopo prioritario e legittimo di aiutare l'organizzazione aziendale, permettendo al *management* di capire quali strumenti comunicativi si rivelano maggiormente idonei alla condivisione di aggiornamenti con i dipendenti.

La continua evoluzione degli strumenti di *web analytics*, tuttavia, ha ampliato la tipologia e la mole di dati che possono essere raccolti e, di conseguenza, delle informazioni che è possibile ottenere. Tali strumenti possono quindi essere usati per conoscere le azioni e le abitudini del dipendente. Se in Internet l'uso degli analytics è regolato dalla normativa sulla *privacy*[23] che impone di rendere anonimi gli indirizzi IP al fine di evitare l'individuazione di un singolo utente e altresì, di trattare i dati soltanto in forma aggregata, nella intranet aziendale, considerata alla stregua di uno strumento di lavoro, tali vincoli vengono meno. Il datore di lavoro potrebbe, dunque, tracciare le azioni compiute da un singolo dipendente nella intranet aziendale e sapere ad esempio se ha letto o meno una specifica normativa, quanto tempo si è soffermato sul documento, analizzare la mappa di calore[24] o addirittura eseguire il *session replay*[25] della sua navigazione nelle risorse della intranet, indipendentemente dal dispositivo usato dal dipendente, che potrebbe persino essere, ad esempio in caso di smart working, di proprietà del dipendente stesso.

Conclusioni

Come scritto in precedenza, il tema del controllo del lavoratore, poiché incide su un diritto riconosciuto dell'individuo, quale quello alla privacy, dovrebbe godere di una speciale attenzione da parte del legislatore onde evitare che la parte datoriale, contrattualmente più forte, approfitti di eventuali lacune normative per estendere il suo controllo oltre i limiti dello stretto necessario.

Dalla modifica eseguita nel 2015 all'art. 4 dello Statuto dei Lavoratori,[26] fino alla recente introduzione emergenziale del lavoro agile semplificato a opera dell'art. 87 del D.L. 18/2020, si è assistito a un ampliamento della possibilità di controllo del lavoratore da parte del datore di

lavoro. L'equilibrio garantito dalla legge si è sbilanciato, dunque, negli ultimi anni, a favore del datore di lavoro, sia per espressa volontà del legislatore che ha eliminato il divieto generale e ampliate le possibilità di controllo sia approfittando della mancanza di regolamentazione delle opportunità di controllo indiretto offerte dalle nuove tecnologie.

Negli ultimi anni, dunque, la situazione del lavoratore risulta notevolmente peggiorata per essenzialmente due cause: la prima scaturisce dall'ampliamento dei controlli datoriali concessa dal legislatore e la seconda dalla nascita di nuove tecnologie che permettorno un controllo sull'attività e sul lavoratore inimmaginabili nel 1970. Inoltre, se gli strumenti di controllo a distanza avevano un costo notevole negli anni '70, oggi strumenti di controllo, anche molto invasivi, sono alla portata anche del più piccolo imprenditore. Sebbene il legislatore dell'epoca abbia avuto una visione lungimirante, estendendo il divieto di controllo a distanza a non precisati "altri strumenti di controllo", tale indicazione si rivela non sufficiente a tutelare adeguatamente i lavoratori, poiché ne restano esclusi gli strumenti di lavoro che permettono un controllo a distanza sull'attività del lavoratore e di fatto rendono superflui ulteriori strumenti di controllo, facendo di fatto venir meno la tutela prevista dall'art. 4 dello Statuto dei Lavoratori. Attualmente, la tutela del lavoratore in smart working nei confronti dei controlli datoriali indiretti appare affidata, più che allo Statuto dei Lavoratori, alla normativa sulla privacy, che ha però un fine teleologico differente rispetto alla tutela dei diritti dei lavoratori. C'è il rischio quindi di non tutelare adeguatamente i lavoratori, dal momento che la platea di coloro che lavorano in smart working è in rapida espansione e le nuove tecnologie rendono i controlli datoriali quasi inscindibili dall'attività lavorativa stessa. Una regolamentazione normativa *ad hoc* appare dunque necessaria e non più rinviabile.

In ultimo, si evidenza che una tematica così delicata, poiché incide direttamente su diritti costituzionalmente garantiti, non dovrebbe essere regolata unicamente dall'accordo individuale tra datore di lavoro e singolo dipendente. Appare opportuno, invece, che essa sia disciplinata nei contratti collettivi. Nel frattempo, sarà anche onere dei sindacati informare e rendere edotto il personale di tali possibilità di controllo indiretto e cercare di porre limiti a eventuali eccessi del datore di lavoro.

NOTE

[1] Un'interpretazione estensiva dei diritti inclusi nella Costituzione fa rientrare la privacy tra i diritti fondamentali della persona, in modo indiretto. Ciò è riconducibile alla teoria dottrinaria cosiddetta della *Costituzione vivente* che vuole che accanto alla Costituzione formale e materiale

vi sia una serie di considerazioni e interpretazioni che ne estendono l'efficacia anche ad aspetti della società che, data la sua continua evoluzione, non sono esplicitamente formalizzati. Sugli scritti inerenti la Costituzione vivente si veda ZAGREBELSKY, G. (2006). La Costituzione vivente, *Storia e memoria*, vol. 15 – Fasc. 1, pp. 69-81.

[2] Articolo 4 legge n. 300/1970.

[3] Articolo 23 D.Lgs. n. 151/2015.

[4] Art. 4 comma 1 L. 300/1970 *È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori*.

[5] Ad esempio, nel trasporto aereo o nel caso di furgoni portavalori.

[6] In Spagna in modo analogo l'Estatuto de los Trabajadores vieta l'uso delle telecamere nei luoghi di riposo e salette di ristoro dei lavoratori e ovviamente negli spogliatoi e nei bagni. Forse la normativa spagnola risulta un po' meno incisiva per quanto riguarda l'uso delle telecamere nei posti di lavoro, che si possono installare anche per finalità di controllo, e non solo come avviene in Italia, nei casi in cui il patrimonio aziendale è a rischio. Ovviamente in Spagna l'uso delle telecamere deve essere bilanciato dalla difesa queste devono essere l'unico modo in cui il datore di lavoro possa operare il proprio controllo, le modalità di utilizzo devono essere strettamente proporzionali alle finalità di tutela, necessita di un'informazione preventiva ai lavoratori sull'uso e le finalità delle registrazioni e il posizionamento di cartellonistica che segnali la presenza di telecamere in un dato luogo.

[7] Art. 8 della Carta dei diritti fondamentali dell'Unione Europea:

> *1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*
> *2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.*
> *3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*

[8] Art. 35 GDPR (regolamento UE/2016/679)

> *Valutazione d'impatto sulla protezione dei dati*
>
> *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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) *una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; Considerando 75 e*

d) *le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione*

Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

[9] Art. 4 legge 300/1970.

[10] Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018 pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018 Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

> *1.Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittiveeffettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gliinteressi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".*
>
> *2.Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente"sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di uncontratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).*
>
> *3.Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraversoreti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della societàdell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche itrattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, diprevisioni di budget, di upgradetecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc*
>
> *4.Trattamenti su larga scala di dati aventi carattere estremamente personale si fa riferimento, fra gli altri, ai dati connessialla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidonosull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazionecomporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia dipagamenti).*

5.Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti.

6.Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

7.Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati dadispositivi wearable; tracciamenti di prossimità come ad es. il wi-fitracking)

8.Trattamenti checomportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9.Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio deidati di consumo di beni digitali con dati di pagamento (es. mobile payment).

10.Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

11.Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

12.Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

[11] In Italia viene chiamata smart working qualsiasi forma di lavoro in remoto, sia essa telelavoro, lavoro agile, lavoro da hub, etc.

[12] Art. 21 L. 81/2017:

> *Potere di controllo e disciplinare 1. L'accordo relativo alla modalita' di lavoro agile disciplina l'esercizio del potere di controllo del datore di lavoro sulla prestazione resa dal lavoratore all'esterno dei locali aziendali nel rispetto di quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300, e successive modificazioni. 2. L'accordo di cui al comma 1 individua le condotte, connesse all'esecuzione della prestazione lavorativa all'esterno dei locali aziendali, che danno luogo all'applicazione di sanzioni disciplinari.*

[13] Quando il datore di lavoro aveva espressamente vietato l'uso del dispositivo per scopi extra-lavorativi.

[14] Art. 7 legge n. 300/1970.

[15] Criteri, in vigore in Italia, elaborati dalla giurisprudenza della Corte di Cassazione (Cass., 10 novembre 2017, n. 26682) della CEDU (CEDU n. 61496/08) e dai provvedimenti del Garante Privacy (Garante Privacy, Newsletter n. 437 del 26 gennaio 2018).

[16] Sulla tematica assumono grande rilievo il provvedimento generale dell'Autorità Garante per la protezione dei dati personali del 1 marzo 2007, il documento di lavoro delle autorità europee di protezione dei dati riunite nel Gruppo dei garanti europei, istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, adottato il 29 maggio 2002, nonché la giurisprudenza della Corte europea dei diritti dell'uomo relativa all'articolo 8 della Convenzione europea dei diritti dell'uomo.

[17] Rimane vietato qualsiasi controllo sulle conversaioni avvenute tramite mail personale, e non aziendale, il cui accesso è avvenuto durante l'orario di lavoro e con strumentazione del datore di lavoro. Il tal caso il datore di lavoro potrà verificare solamente l'accesso dell'IP del computer al server di posta.

[18] Art. 15 Costituzione italiana.

[19] La geolocalizzazione risulta possibile solo con gli smartphone di nuova generazione. Per quanto riguarda i cellulari precedenti, è possibile risalire alla loro posizione approssimativa solo attraverso le celle, ma questi ultimi sono dati a cui ha accesso, generalmente, solo la magistratura.

[20] Art. 4 legge 300/70 I comma.

[21] Art. 4 legge 300/70 I comma.

[22] D. Lgs. 66/2003.

[23] Regolamento UE/2016/679.

[24] La mappa di calore è un grafico che evidenza attraverso una scala di colori, le porzioni di pagina web più o meno cliccate dagli utenti.

[25] Il *session replay* è uno strumento avanzato di *web analytics* che permette di vedere una ricostruzione visuale della navigazione eseguita dagli utenti su una pagina.

[26] Art. 23 D.Lgs. 151/2015.

Bibliografía

ALVINO, I. (2016). I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy, *LLI*, vol. 2, n. 1, 7.

INGRAO, A.(2018). *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Bari: Cacucci Editore.

RUSSO, A. e TUFO, M. (2016). I controlli preterintenzionali: la nozione, in LEVI, A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo statuto dei lavoratori dopo il jobs act*, Giuffrè, 54.

STANCHI, A.(2016). Controlli del datore sul pc aziendale e privacy, in *Guida al Lavoro*, n. 10, 31.

STAROPOLI, P. (2017). Smart working e controllo sul lavoratore tramite gli strumenti di lavoro, in *Ipsoa*, Wolters Kluwer, 5/2017, 297.

TULLINI, P. *(2009).* Comunicazione elettronica, potere di controllo e tutela del lavoratore, in *Rivista Italiana di Diritto del Lavoro*, 1/2009, 485.

IDEM. (2011). Videosorveglianza a scopi difensivi e utilizzo delle prove del reato comune del dipendente, in *Rivista Italiana di Diritto del Lavoro*, vol. 2, 85.

ZAGREBELSKY, G. (2006). La Costituzione vivente, *Storia e memoria*, vol. 15 – Fasc. 1, pp. 69-81.