UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M. FANNO"

DIPARTIMENTO DI AFFERENZA DEL RELATORE: DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

"I CONTROLLI DIFENSIVI OGGI"

RELATORE:

CH.MO/A PROF./SSA BARBARA DE MOZZI

LAUREANDO/A: RACHELE DURELLO

MATRICOLA N. 2001140

ANNO ACCADEMICO 2022 – 2023

APPENDICE

Dichiarazione di autenticità

Dichiaro di aver preso visione del "Regolamento antiplagio" approvato dal Consiglio del Dipartimento di Scienze Economiche e Aziendali e, consapevole delle conseguenze derivanti da dichiarazioni mendaci, dichiaro che il presente lavoro non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere. Dichiaro inoltre che tutte le fonti utilizzate per la realizzazione del presente lavoro, inclusi i materiali digitali, sono state correttamente citate nel corpo del testo e nella sezione 'Riferimenti bibliografici'.

I hereby declare that I have read and understood the "Anti-plagiarism rules and regulations" approved by the Council of the Department of Economics and Management and I am aware of the consequences of making false statements. I declare that this piece of work has not been previously submitted – either fully or partially – for fulfilling the requirements of an academic degree, whether in Italy or abroad. Furthermore, I declare that the references used for this work – including the digital materials – have been appropriately cited and acknowledged in the text and in the section 'References'.

Firma (signature) Rachele Durello

Indice

Introduzione

Il potere di controllo, che sarà fulcro di questo studio, non era stato disciplinato nel Codice Civile del 1942, essendo considerato, a quell'epoca, una conseguenza diretta del potere direttivo del datore di lavoro. Solo nel 1970, con la stesura del cd Statuto dei Lavoratori (legge 300/70), il legislatore decide di porre dei limiti all'esercizio di questo potere, bilanciando gli interessi contrapposti del creditore e del debitore della prestazione lavorativa. Con l'articolo 4 veniva tracciato un confine oltre il quale il datore di lavoro non poteva muoversi e dove venivano tutelati quei diritti fondamentali dell'uomo, il diritto alla libertà e alla dignità, già presenti nella nostra Costituzione (art. 41). L'esercizio del controllo a distanza viene limitato prevedendone, da un lato, l'assoluto divieto e dall'altro, qualora fosse stato una possibile conseguenza di esigenze aziendali qualificate, veniva richiesta l'autorizzazione sindacale. Unica eccezione veniva fatta per quei controlli cd difensivi, diretti ad accertare illeciti extracontrattuali (Capitolo I).

Tuttavia, una norma redatta in un momento storico in cui gli strumenti tecnologici non erano ancora entrati a far parte dell'ambito lavorativo, non era in grado di tenere il passo dell'evoluzione tecnologica e la sua obsolescenza obbligò il legislatore a riformarla. (Capitolo II). Così con il decreto legislativo n. 151 del 2015, vengono introdotte delle novelle. Diverse modalità di installazione e utilizzo vengono definite per gli strumenti di controllo e per quelli di lavoro e il bilanciamento degli interessi si traduce nella possibilità da parte del datore di effettuare controlli e nel diritto del lavoratore di essere preventivamente informato. Il legislatore inoltre va a definire le modalità di trattamento dei dati raccolti, facendo riferimento alla disciplina che era stata emanata in materia di *privacy* dal Garante.

L'evoluzione tecnologica, però, non si è fermata all'introduzione dei *personal computer* o degli *smartphone* in azienda, ma ha continuato a diffondere piattaforme e strumenti sempre più pericolosi per quanto riguarda la possibilità di controllo (Capitolo III). Così, oggi, il datore di lavoro è in grado di immagazzinare un numero enorme di dati riguardanti non solo l'esatto adempimento della prestazione, ma anche la vita privata del lavoratore ponendo nuovi interrogativi sul futuro.

Capitolo I: Il vecchio articolo 4 dello Statuto dei Lavoratori: i controlli difensivi

1.1 I primi limiti in materia di controlli a distanza

Negli anni settanta il legislatore aveva sentito l'esigenza di limitare il potere del datore di lavoro in materia di controlli a distanza per tutelare la riservatezza del lavoratore e la dignità e la libertà[1] di quest'ultimo durante lo svolgimento della sua prestazione lavorativa. Il legislatore, quindi, aveva scelto di vietare, in via assoluta, un controllo continuativo e occulto, a distanza, sull'attività del lavoratore attraverso l'impiego di impianti audiovisivi o apparecchiature tecnologiche, permettendo allo stesso tempo, previo accordo con le rappresentanze sindacali in azienda o, in mancanza, con l'autorizzazione dell'Ispettorato del lavoro, l'impiego di questi strumenti per soddisfare esigenze organizzative e produttive o per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Il legislatore aveva quindi ammesso l'ipotesi di impiegare le apparecchiature per le fattispecie sopra individuate dalle quali poteva derivare un controllo sull'attività del lavoratore, il cd. controllo preterintenzionale.

1.2 La categoria dei c.d. controlli difensivi: evoluzione dell'orientamento giurisprudenziale

Per quanto riguarda invece la categoria dei cd. controlli difensivi, il legislatore non aveva identificato delle precise fattispecie e, per questo motivo, la giurisprudenza si era pronunciata numerose volte con pareri discordarti che, oggi, possono essere riassunti in due categorie.
Il primo orientamento può essere descritto facendo riferimento a una sentenza risalente al 2002[2] nella quale la Corte aveva escluso i controlli difensivi dall'ambito di applicazione dell'art. 4 legge 300/1970. Aveva quindi attuato una distinzione tra i cd. controlli preterintenzionali e i cd. controlli difensivi. I primi erano quelli volti ad individuare comportamenti illeciti da parte del lavoratore facenti parte della prestazione lavorativa, già tutelati dal secondo comma, articolo 4 legge 300/1970 che proteggeva il dipendente attraverso il necessario accordo con le rappresentanze sindacali o con l'ispettorato del lavoro. I secondi erano quelli volti ad individuare comportamenti illeciti da parte del lavoratore estranei al rapporto di lavoro, e che, di conseguenza, erano esclusi dall'ambito di applicazione dell'articolo 4. Aveva infatti affermato che: "ai fini del divieto di utilizzo di apparecchiature per il controllo a distanza…, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dall'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi) …".

[1] Diritto tutelato dall'articolo 41 della Costituzione
[2] Cass. 3 aprile 2002, n. 4746

Questa e altre sentenze simili[3] suscitarono non poche perplessità in gran parte della dottrina, la quale (secondo orientamento) oppose due argomentazioni. In primo luogo sarebbe stato inesatto escludere sempre i controlli difensivi dai limiti posti dal secondo comma dell'articolo 4, in quanto l'utilizzo di apparecchiature per il controllo di eventuali illeciti da parte del lavoratore, consentiva anche un controllo indiretto (sebbene indiretto, pur sempre un controllo), sulla prestazione lavorativa dei dipendenti per quanto attinente ai tempi e ai contenuti dell'attività. Inoltre la legittimità del controllo si sarebbe potuta accertare solo *ex post* dal momento che, qualora il lavoratore non avesse commesso illeciti, il controllo si sarebbe dovuto ritenere illegittimo e le informazioni inutilizzabili ai fini sanzionatori. L'esigenza di poter verificare condotte illecite da parte dei lavoratori non poteva "assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore"[4].

Successivamente la giurisprudenza si discostò da quanto affermato nella sentenza n. 4746 del 2002, riconoscendo sì la categoria dei controlli difensivi, ma, nel caso in cui tali controlli permettessero un'ispezione sull'attività del dipendente, si sarebbe dovuta espletare la procedura dettata dal secondo comma, articolo 4. Questo a garanzia della dignità e della riservatezza del lavoratore.

Il cambiamento interpretativo è stato poi espressamente riconosciuto dalla Cassazione[5]. I giudici di legittimità hanno affermato che, quando dall'utilizzo dello strumento per accertare l'illecito possa derivare anche un controllo sull'esatto adempimento della prestazione del lavoratore, allora si applica il secondo comma dell'articolo 4 dello Statuto ed è necessaria la predisposizione di un'adeguata informativa seguendo i "principi di finalità, necessità, proporzionalità, pertinenza e non eccedenza[6]". Quando invece i controlli sono diretti ad accertare illeciti che possano pregiudicare "beni estranei al rapporto di lavoro" come quelli lesivi del patrimonio e dell'immagine dell'azienda, allora non è necessario espletare la procedura dettata dal secondo comma[7].

In pratica è però difficile riuscire a distinguere tra questi due casi ed è ancora più difficile individuare comportamenti illeciti senza acquisire informazioni sull'adempimento dell'attività lavorativa del dipendente.

1.3 Il concetto di patrimonio aziendale

Un ulteriore problema sorge nel momento in cui si prova a definire concretamente il concetto di "patrimonio aziendale". Come osservato da Ilario Alvino[8] rientrerebbero nella definizione "non solo

---

[3] Cass. 19 luglio 1985, n. 4271; Cass. 25 gennaio 1992, n. 829; Cass. 4 aprile 2012, n. 5371 e Cass. 23 febbraio 2012, n. 2722

[4] Cass. 17 luglio 2007, n. 15892

[5] in Cass. 18 aprile 2012, n. 16622

[6] Linee-guida in materia di trattamento di dati personali

[7] Tra le altre Cass. 17 luglio 2007, n. 15892; Cass., Sez. L, n. 4375 del 2010 e Cass., Sez. L., n.9904 del 2016

[8] In "L'art. 4 Stat. Lav. alla prova di internet e della posta elettronica", Diritto delle Relazioni Industriali, Numero 4/XXIV – 2014, pag. 1015-1016

i beni materiali dei quali sia composto, ma anche il complesso dei rapporti che sono essenziali per lo svolgimento dell'attività produttiva", in una lettura, quindi, di senso ampio. In questo senso è interessante una pronuncia della Corte di Cassazione[9] che ben descrive la portata del concetto di "patrimonio aziendale". In questa sentenza, un dipendente di un istituto bancario aveva divulgato a terzi, attraverso la casella di posta elettronica della banca, informazioni sensibili di un cliente che aveva poi utilizzato per eseguire delle operazioni finanziare a proprio vantaggio. Per questo motivo il lavoratore era stato dapprima sospeso cautelarmente fino alla conclusione degli accertamenti ispettivi, poi licenziato. Lo stesso aveva quindi proposto ricorso adducendo, tra gli altri motivi, che il controllo della posta elettronica era stato fatto in violazione dell'articolo 4 dello Statuto in quanto mancava l'accordo con le rappresentanze sindacali aziendali o l'autorizzazione dell'Ispettorato del lavoro. Il Collegio affermò invece che, in questo caso, il controllo era estraneo al campo di applicazione dell'articolo 4 e in particolare "entrava in gioco il diritto del datore di lavoro di tutelare il proprio patrimonio, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico. Questa forma di tutela egli poteva giuridicamente esercitare con gli strumenti derivanti dall'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale.[10]"

La Suprema Corte aveva poi chiarito che, perché il controllo rientrasse nella categoria dei c.d. controlli difensivi, era necessaria la presenza di "elementi di fatto tali da raccomandare l'avvio di un'indagine retrospettiva"[11]. Pertanto il datore di lavoro, prima di poter avviare controlli fuori dall'ambito di applicazione del secondo comma, articolo 4, doveva avere sospetti fondati su un possibile illecito commesso da uno dei dipendenti e, solo a quel punto, poteva ritenersi corretta la raccolta di informazioni (non finalizzate quindi al controllo sull'attività del lavoratore ma alla salvaguardia del patrimonio aziendale).

Nonostante le continue pronunce della Corte, la corretta applicazione di tale norma si rimetteva di volta in volta alle decisioni dei giudici che facevano riferimento ai casi specifici.

1.4 Statuto dei lavoratori e Codice della *privacy*

Per concludere questo primo capitolo, è opportuno riportarsi alla disciplina sul trattamento dei dati personali[12] e alle linee-guida del Garante in materia di utilizzo della posta elettronica e di internet, emanate con delibera n. 13/2007. Tali linee-guida, vincolanti nei confronti dei datori di lavoro, rispondevano all'esigenza "di prescrivere ai datori di lavoro alcune misure, necessarie ed opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il

[9] Cass. 23 febbraio 2012, n. 2722. Si veda anche Cass. 23 febbraio 2010, n. 4375
[10] Cass. 23 febbraio 2012, n. 2722, cit.
[11] Cass. 17 luglio 2007, n. 15892, cit.
[12] In seguito alle direttive 95/46/CE e 2002/58/CE. Oggi sostituite dal Regolamento 2016/679 UE

corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete internet"[13]. Obiettivo era quello di limitare il potere di controllo che, sebbene esercitato nel rispetto del secondo comma, articolo 4 dello Statuto, poteva far sì che il datore di lavoro venisse conoscenza di dati personali del lavoratore[14]. È comunque importante sottolineare che le disposizioni dettate dal Garante non sostituiscono quelle delineate nel secondo comma, articolo 4 legge 300/70, ma devono ritenersi complementari[15] operando su un diverso piano rispetto a quelle dello Statuto. Al punto 5 delle linee guida viene precisato che il trattamento dei dati, che derivi dall'utilizzo di strumenti di controllo impiegati "per esigenze produttive o organizzative ovvero per la sicurezza del lavoro", può essere lecito se è espletata la procedura prevista dal secondo comma, articolo 4 dello Statuto. Nel caso contrario le informazioni acquisite non potranno essere usate per la contestazione dell'illecito.
Affinché il controllo sull'utilizzo di internet e della posta elettronica sia corretto, il Garante identifica quattro principi cui il datore di lavoro dovrà attenersi.
Il primo principio è il principio di necessità, secondo il quale il datore di lavoro deve configurare gli strumenti informatici in modo da ridurre al minimo l'impiego di informazioni di carattere personale dei lavoratori, utilizzando, per quanto possibile, dati anonimi.
Il secondo è il principio di correttezza, a cui si collega quello di trasparenza. Il datore di lavoro ha l'onere di informare i dipendenti sulle "caratteristiche essenziali dei trattamenti" e, come specificato anche dal punto 3.1, è tenuto ad informare i lavoratori sulle modalità d'uso degli strumenti informatici, di internet e della posta elettronica e sulle modalità con le quali verranno effettuati controlli, se necessari.
Infine, secondo i principi di non eccedenza e di pertinenza (terzo e quarto principio) i dati devono essere trattati "nella misura meno invasiva possibile". Il Garante invita il datore a effettuare prioritariamente un controllo su dati aggregati ed a emettere un "avviso generalizzato" sulle anomalie riscontrate, ricordando le giuste modalità di impiego degli strumenti. Solo in caso di ripetute anomalie, si potrà procedere con un controllo. Inoltre vieta la possibilità di effettuare "controlli prolungati, costanti o indiscriminati". I dati non necessari devono perciò essere cancellati "periodicamente ed automaticamente"; una dilazione nei tempi di conservazione può avvenire solo per le fattispecie esplicitamente indicate (esigenze tecniche o di sicurezza del tutto particolari; indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria; obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria).

[13] Linee-guida del Garante per posta elettronica e internet, delibera n. 13/2007, cit.
[14] Punto 1.1 delle linee-guida
[15] L'articolo 114 del codice della privacy fa esplicitamente salvo l'articolo 4 dello Statuto

Nonostante l’introduzione di questa ulteriore specificazione in materia di controlli, le sempre nuove e più complesse tecnologie richiedevano un rimodellamento della disciplina che potesse rendere la norma universale e di più immediata applicazione. Questo sarà argomento del capitolo secondo.

Capitolo II: La nuova disciplina dei controlli a distanza: le novità del Jobs Act

2.1 Le carenze del vecchio articolo 4

Di una riforma dell'articolo 4 dello Statuto dei lavoratori se ne discuteva fin dagli anni ottanta. La principale critica mossa era sicuramente quella che la norma, nata quando le tecnologie impiegate per l'attività lavorativa erano agli albori, non riusciva, come scrive Maria Teresa Salimbeni, a "regolare il nuovo che avanza".[16] Si sentiva quindi la necessità di un bilanciamento tra l'esigenza di vincolare ulteriormente il datore di lavoro e la protezione della già citata dignità e riservatezza del lavoratore. Per quanto riguarda il datore di lavoro egli poteva eseguire un controllo molto più pervasivo e massivo sull'attività del lavoratore a causa dei nuovi strumenti informatici (intrinsecamente dotati di elementi in grado di incamerare dati) essenziali per l'adempimento della prestazione. Allo stesso tempo il datore era maggiormente a rischio a causa delle nuove "opportunità" di commettere illeciti da parte dei lavoratori.

Inoltre era necessario superare le incertezze applicative proprie dell'articolo 4 dello Statuto, che, come ho dimostrato nel capitolo precedente, non era chiaro e la sua interpretazione si rimetteva di volta in volta ai singoli giudici.

Così nel 2014, con la legge delega n. 183[17], attuata con il d.lgs. n. 151 del 2015 il legislatore prevedeva: "la revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore". Perciò l'articolo 4 viene completamente riscritto, modificando per prima cosa la struttura, poi i beni tutelati e infine la garanzia procedurale.[18]

---

[16] In "La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore", RIDL, 2015, I, pag. 589

[17] Art. 1, co. 7, lett. f)

[18] "Art. 4 (Impianti audiovisivi e altri strumenti di controllo). - 1. Gli impianti audiovisivi e gli altri strumenti 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 rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali. 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. 3. Le informazioni raccolte ai sensi dei commi 1 e 2 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 decreto legislativo 30 giugno 2003, n. 196"

2.2 Il nuovo articolo 4, comma 1

La prima parte del primo comma non introduce novità (ma semplicemente cambia la formulazione della frase). Scompare il divieto esplicito di utilizzo di impianti audiovisivi e altre apparecchiature, che nel nuovo testo sono sostituiti da "impianti audiovisivi e altri strumenti", per finalità di controllo dei lavoratori. Per quegli strumenti, dai quali derivi anche la possibilità di controllo, affinché possano essere installati, il legislatore individua delle fattispecie qualificate che tutelano sia la sfera del datore di lavoro ("esigenze organizzative e produttive" e "patrimonio aziendale") sia quella dei soggetti presenti in azienda ("sicurezza del lavoro"). L'illecito nasce nel momento in cui gli strumenti, dai quali derivi anche la possibilità di controllo, vengono solamente installati senza il necessario accordo e la violazione è condotta punibile in sede penale.

L'unica novella è l'introduzione del concetto di patrimonio aziendale tra le ipotesi ammesse. Questa modifica, secondo alcuni[19], dimostrerebbe la volontà di superare definitivamente e allo stesso tempo di trasformare la categoria dei cd. controlli difensivi in un controllo co-determinato. Questa categoria ammetteva, tra le diverse ipotesi, che per la tutela del patrimonio aziendale non fosse necessaria la procedura dettata dal secondo comma, ex articolo 4 (rendendo così il controllo difensivo un controllo *extra legem*). Oggi quindi sembrerebbe errato ritenere che si possa attivare un controllo difensivo in quanto il controllo investirebbe l'ordinaria attività lavorativa e non solo l'attività illecita. Allo stesso modo una qualificazione *ex post* del controllo ricadrebbe senza dubbio nell'applicazione del primo comma dal momento che l'acquisizione e l'utilizzazione dei dati avverrebbe sempre sulla prestazione in quanto tale. I controlli difensivi attuati per la salvaguardia del patrimonio aziendale sono quindi ritenuti legittimi a condizione che sia rispettato l'*iter* previsto dal primo comma dell'articolo 23 del *Jobs Act* e che siano rispettate le linee guida dettate dal Garante in tema di privacy. Il datore di lavoro dovrà specificare nell'informativa data al lavoratore (secondo il principio di "limitazione delle finalità)[20] sia che i dati potranno essere trattati per la tutela del patrimonio aziendale sia quali saranno le conseguenze disciplinari in caso di accertamento di un comportamento illecito. Inoltre si ritiene che, affinché il controllo sull'attività lavorativa sia legittimo e che di conseguenza siano legittime le sanzioni disciplinari, sia sufficiente la mera presenza di un pericolo per l'immagine dell'azienda a prescindere dal verificarsi del danno.[21] Oggi, perciò, si ritiene che il controllo occulto sia vietato. Secondo alcuni[22], comunque, sarebbe errato pensare che la categoria dei controlli difensivi sia eliminata del tutto dal momento che, nel caso in

---

[19] Tra gli altri Riccardo del Punta in "La nuova disciplina dei controlli a distanza sul lavoro", RIDL, 2016, I, pag. 97

[20] Art. 5, par. 1, lett. b

[21] Così Alessandra Ingrao in "Il controllo disciplinare e la privacy del lavoratore dopo il *Jobs Act*, RIDL, 2017; II, pag. 51

[22] Tra gli altri Emanuele Dagnino in "Tecnologie e controlli a distanza", Diritto delle Relazioni Industriali, Numero 4/XXV – 2015, pag. 1003 e Arturo Maresca in "Controlli tecnologici e tutele del lavoratore", RIDL, 2016, I, pag. 525

cui il controllo sia mirato ad accertare condotte illecite estranee al rapporto di lavoro, si potrebbe parlare di controllo difensivo in senso stretto. Questo potrebbe avvenire, ad esempio, nel caso in cui sia installato un *software* che sia in grado di identificare esclusivamente reati informatici e che non riguardi quindi l'attività lavorativa nel suo complesso.

La seconda parte del primo comma velocizza la procedura per raggiungere l'accordo sindacale per l'installazione degli strumenti. Dice infatti che "nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale". Sicché, trattandosi di un modello di competenza sindacale concorrente e multilivello, per le imprese territorialmente articolate non è necessario confrontarsi con ciascuna unità produttiva, ma è sufficiente raggiungere un accordo con un'associazione comparativamente più rappresentativa sul piano nazionale che poi varrà per tutte le unità. Inoltre in mancanza di accordo, l'impresa potrà ricevere l'autorizzazione per installare gli impianti dalla Direzione territoriale del lavoro o, nel caso di imprese con più unità produttive, dal Ministero del lavoro e delle politiche sociali. Per quanto riguarda questo periodo finale l'unico cambiamento rispetto al vecchio testo sta nel fatto che non viene espressamente affermato che l'Ispettorato del lavoro all'occorrenza possa dettare "le modalità d'uso di tali impianti[23]". Alcuni[24] ritengono che non ci sia motivo di ritenere che il legislatore abbia voluto eliminare la possibilità di aggiungere ulteriori vincoli da quelli stabiliti dal datore. Altri[25] invece ritengono che l'Ispettorato possa solo esprimersi riguardo alla meritevolezza e alla effettiva presenza delle esigenze fissate dal primo comma.

2.3 Strumenti di controllo e strumenti di lavoro

Proseguendo, il secondo comma non offre la stessa chiarezza del comma precedente. Affermando infatti che "la disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze" si è aperta una discussione su quali fossero effettivamente gli strumenti fuori dall'ambito di applicazione del comma citato, dal momento che, talvolta, è difficile definire precisamente ciò che serve per rendere più sicura l'attività lavorativa e ciò che serve per rendere più sicura l'organizzazione del lavoro. Ci sono diverse opinioni in merito a quali elementi si dovrebbe tener conto nell'attuare questa distinzione. Alcuni[26] ritengono che sia necessario che lo strumento renda più efficiente il lavoro. Altri[27] che sia indispensabile per eseguire l'attività lavorativa e che quindi vi

[23] Comma 2, ex articolo 4, Statuto dei lavoratori
[24] Tra gli altri Riccardo del Punta in "La nuova disciplina dei controlli a distanza sul lavoro", RIDL, 2016, I, pag. 99
[25] Tra gli altri Alessandra Ingrao in "Il controllo disciplinare e la privacy del lavoratore dopo il *Jobs act*", RIDL, 2017, II, pag. 51
[26] Ilario Alvino, "I nuovi limiti", pag. 27
[27] Riccardo del Punta, "La nuova disciplina dei controlli a distanza sul lavoro", RIDL, 2016, I, pag. 100

debba essere una stretta correlazione tra i *device* e le mansioni svolte dal lavoratore. Altri ancora attribuiscono importanza al ruolo che assume il lavoratore in relazione a questi strumenti, nel senso di essere in grado di attivare o disattivare la funzione di controllo.
In generale per strumenti si intendono non soltanto la parti *hardware* ma anche i programmi di *software* scaricati. Queste due componenti hanno una diversa funzione rispetto all'attività lavorativa e lo stesso Ministero ha sottolineato che si dovrà procedere alla scomposizione, di volta in volta, delle diverse funzionalità di ogni *device* e, nel caso in cui vi sia la possibilità di controllare l'attività lavorativa rispondente a una delle esigenze individuate dal legislatore, si ricadrà nel comma 1.
Inoltre si dovrà tener conto dell'utilizzo che ne fa il dipendente in relazione alle mansioni effettivamente svolte. Per portare degli esempi concreti: telecamere installate sui veicoli aziendali oppure sistemi in grado di monitorare gli accessi a internet o la durata della connessione o ancora sistemi di registrazione delle chiamate con i clienti rispondono a esigenze di sicurezza dell'impresa e quindi dovranno essere installati previo accordo sindacale. Invece, per quanto riguarda il *computer* o il *badge* che registri l'orario di entrata e uscita dal lavoro sarebbe improponibile richiedere l'espletazione della procedura di cui al comma 1. In conclusione dell'analisi del secondo comma è importante sottolineare quanto afferma il legislatore: "non si autorizza nessun controllo a distanza; piuttosto, si chiariscono solo le modalità per l'utilizzo degli strumenti tecnologici impiegati per la prestazione lavorativa ed i limiti di utilizzabilità dei dati raccolti con questi strumenti" al fine di fugare ogni dubbio in merito alle possibili interpretazioni di questo comma.

2.4 Vincoli e adeguata informativa

Infine il terzo comma definisce le modalità di utilizzo dei dati raccolti ("a tutti i fini connessi al rapporto di lavoro") che va ad incidere non solo sul potere di controllo ma anche su quello disciplinare e a tutti gli altri connessi alla gestione del rapporto (come la valutazione della produttività a fini retributivi). Grazie a queste delucidazioni si va a colmare una lacuna del vecchio art. 4 che non definiva concretamente le modalità di utilizzo dei dati.
La raccolta dei dati, innanzi tutto, dovrà avvenire nel rispetto del comma 1, articolo 4 quindi previo accordo sindacale, altrimenti questi non saranno utilizzabili anche nel caso si riscontrino illeciti da parte del lavoratore. L'altra condizione è 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 decreto legislativo 30 giugno 2003, n. 196"[28]. Come già esposto nel capitolo precedente i vincoli prescritti nell'articolo 4 e quelli del d.lgs. 30 giugno 2003, n. 196 non si sovrappongono ma si integrano a formare la complessiva tutela del lavoratore in materia di controlli a distanza, fondata sulla trasparenza e sulla salvaguardia delle dignità e della libertà della persona.

[28] Sostituito dal regolamento 2016/679/UE, armonizzato dal d.lgs. n. 101/2018

2.5 Un breve riassunto

Per riassumere i punti più importanti della riforma possiamo dire che: rimane in vita il divieto di utilizzare impianti audiovisivi o altre apparecchiature per controllare a distanza il lavoratore; l'installazione di strumenti dai quali derivi la possibilità di controllo può avvenire solo per le fattispecie individuate dal legislatore (esigenze produttive o organizzative, per la tutela del patrimonio aziendale e per la sicurezza del lavoro) e previo accordo sindacale o previa autorizzazione dell'Ispettorato del Lavoro; viene attuata una distinzione tra strumenti di controllo e strumenti per prestare l'attività lavorativa e per i secondi non è necessario alcun accordo; viene introdotta la disciplina per l'utilizzo dei dati raccolti che vieta il controllo occulto e richiede che vengano rispettate le disposizioni dettate dal primo comma e dalle linee guida del Garante in materia di *privacy.*

Capitolo III: Controlli difensivi e tecnologia: social network e braccialetto elettronico

3.1 L'inarrestabile evoluzione tecnologica

Dopo aver ripercorso l'evoluzione normativa riguardo l'articolo 4 soffermandomi sui concetti di controllo a distanza e controllo difensivo, vorrei, in questo terzo e ultimo capitolo, analizzare due nuovissime tecnologie che pongono non pochi interrogativi riguardo al futuro dei controlli stessi: i *social network* e il braccialetto elettronico.

Oggi la quantità di dati personali che si possono acquisire sugli altri è davvero notevole e non è nemmeno così complicato dal momento che ormai tutti viviamo in una società sempre connessa, in cui vita reale e vita virtuale si intrecciano. A causa dell'inarrestabile evoluzione tecnologica il controllo è diventato apparentemente meno invadente, ma realmente è un'onda che sommerge tutti. Possiamo parlare di sistemi di controllo "passivi" perché i dati vengono sì spontaneamente condivisi, ma sono in grado di offrire un quadro completo delle abitudini, delle opinioni e addirittura della personalità di ciascuno di noi. Inoltre sono in grado di collocare ciascun individuo in una dimensione spazio-temporale a causa della localizzazione GPS e della rilevazione oraria permesse dalla maggioranza delle piattaforme. Come suggerisce Laura Tebano il controllo avviene attraverso la cd. "dataveglianza" ossia "la sorveglianza basata sulla ricostruzione di tracce lasciate nei vari ambienti virtuali"[29].

3.2 Social network: strumenti di lavoro o di controllo?

I *social network*, oltre ad essere un potente strumento di comunicazione, possono avere implicazioni negative per gli utenti che li utilizzano, soprattutto per coloro che, condividendo gran parte della propria vita, si dimenticano della possibile invasione della *privacy*. Per la categoria dei lavoratori subordinati, in particolare, è importante ricordare che il datore di lavoro può venire a conoscenza, attraverso i contenuti postati nelle piattaforme *social*, di fatti sgraditi all'azienda, idonei a giustificarne un licenziamento. Prima di portare ad esempio alcune sentenze, vorrei però concentrarmi su una distinzione che è doveroso fare.

I *social network* possono configurarsi sia quale strumento di lavoro dematerializzato sia quale strumento di controllo (dalla prospettiva, in questo caso, del datore). Nel caso in cui il lavoratore utilizzi il *social media* come strumento per prestare l'attività lavorativa (si pensi ad esempio a tutte quelle nuove figure aziendali che sono emerse negli ultimi anni, quali il *social media manager,* responsabile delle campagne pubblicitarie o il *content creator*, incaricato di creare contenuti per l'azienda), si ricade nel secondo comma dell'articolo 4. Perciò non sarà necessario l'accordo sindacale per dotare il lavoratore di tali strumenti, ma sarà sufficiente che il datore lo informi sulle modalità di utilizzo attraverso l'apposita informativa e della possibilità di controllo nel caso in cui si

[29] Laura Tebano in "La nuova disciplina dei controlli a distanza", RIDL, 2016, I, pag. 347

riscontrino anomalie. I dati acquisiti saranno utilizzabili a tutti i fini connessi al rapporto di lavoro (comma 3, articolo 4) se raccolti nel rispetto di quanto previsto dal Garante nel Codice della *Privacy* secondo i principi di trasparenza e informazione, prevenzione (controllo quale *extrema ratio*), e proporzione (divieto assoluto di un controllo prolungato e indiscriminato). Nel caso in cui questi limiti non vengano rispettati, i dati saranno inutilizzabili.

Passiamo ora al caso in cui il *social* faccia parte della sfera privata del lavoratore e che quindi quest'ultimo lo utilizzi come piattaforma per condividere la sua vita. Innanzitutto se il profilo è privato i contenuti postati sono da ritenersi riservati e quindi, nel caso in cui il datore venga a conoscenza di fatti che potrebbero compromettere il rapporto di lavoro, non potrà utilizzarli come prove. Se, invece, il profilo è pubblico, quindi visibile "agli amici degli amici"[30], chiunque ha il potere e il diritto di visualizzare ciò che viene pubblicato, anche il datore di lavoro. I *post* infatti, pubblicati nelle piattaforme come *Facebook, Instagram* o *Twitter*, sono spesso utilizzati quali prove di inadempimento della prestazione o inadempimento dell'obbligo di diligenza e buona fede[31] e perciò possono configurarsi come causa legittima di licenziamento. Si possono far rientrare questi controlli nella categoria dei cd difensivi dal momento che accertano illeciti extracontrattuali perpetrati nei confronti del datore di lavoro o dell'azienda. Il controllo potrà avvenire in una maniera che si può definire occulta nel senso che, il datore di lavoro (ficcanaso o diffidente), potrà controllare i profili pubblici dei suoi dipendenti ogniqualvolta lo vorrà, in modo legittimo.

3.3 Alcune sentenze

Proporrò ora alcune sentenze che sono esemplificative dei casi descritti sopra.

Il primo caso che voglio portare è quello di un controllo del profilo *Facebook* di un dipendente in malattia (violazione della diligenza e della buona fede). La sentenza risale a marzo 2018[32]. Un datore di lavoro scopre che un suo dipendente, assente per malattia, aveva partecipato, nel mentre, a un concerto, suonando egli stesso in una band la fisarmonica. Aveva appreso tale notizia da una foto, postata dallo stesso su *Facebook*, e da un'altra foto pubblicata in una locandina di un giornale di stampa locale e per questo motivo gli aveva intimato il licenziamento riportando, tra gli altri motivi, che l'attività extralavorativa era da ritenersi incompatibile con lo stato di malattia (in

---

[30] Nella relazione per il 2010, il Garante, a pag. 112, porta come esempio quello di un lavoratore che aveva postato su *Facebook* delle foto che lo ritraevano nei locali aziendali nella quali, sullo sfondo, comparivano delle immagini coperte da segreto industriale e, per questo motivo, era stato licenziato. Nonostante il dipendente affermasse il carattere privato del suo *account*, l'Autorità riteneva lecito l'utilizzo di tali fotografie dal momento che la consultazione del profilo era concesso anche a "contatti scelti dagli amici dell'interessato, quindi a una cerchia di utenti sostanzialmente indeterminabile".

[31] Nell'ordinanza del Tribunale di Bergamo del 24 Dicembre 2015 viene ribadito che: "esistono condotte concernenti la vita privata del lavoratore che possono in concreto risultare idonee a ledere irrimediabilmente il vincolo fiduciario che connota il rapporto di subordinazione, nel senso che mostrano di riflettersi sulle funzionalità del rapporto compromettendo le aspettative di un futuro affidabile adempimento dell'obbligazione lavorativa."

[32] Cass. 13 Marzo 2018, n. 6047

particolare la lombo sciatalgia) e che quindi quell'attività poteva provocare un ritardato rientro a lavoro[33]. Il dipendente aveva proposto ricorso sottolineando il fatto che, dal momento che aveva suonato da seduto, l'attività poteva ritenersi compatibile con lo stato di malattia perché non aveva richiesto alcuno sforzo fisico. La Corte, dopo aver preso in esame i diversi motivi, arriva a dichiarare accertata la simulazione di malattia, anche per il fatto che nella foto postata in *Facebook*[34] il lavoratore suonava in piedi.

Il secondo caso è quello di un dipendente che posta frasi denigratorie nei confronti del datore o dell'azienda nel suo *account social* o in un gruppo (inadempimento extracontrattuale). La prima sentenza è recente e risale al 2021[35]. Un dipendente pubblica su *Facebook* un *post* fortemente denigratorio in cui offende sia i suoi diretti superiori sia i vertici aziendali e per questo motivo viene licenziato per giusta causa. Il lavoratore si difende dicendo che il *post* era indirizzato solamente ai suoi "amici" e, perciò, l'accusa di diffamazione o denigrazione infondata. La Corte afferma che "il mezzo utilizzato … è, infatti, idoneo … a determinare la circolazione del messaggio tra un gruppo indeterminato di persone" ed è tale da ledere irrimediabilmente il rapporto fiduciario tra lavoratore e datore di lavoro.

Una sentenza analoga è la n. 10280 del 27 aprile 2018 in cui un dipendente aveva pubblicato un messaggio diffamatorio nei confronti dell'azienda sulla sua bacheca virtuale di Facebook. Anche in questo caso la Corte aveva ritenuto legittimo il licenziamento in quanto il messaggio era in grado di raggiungere un numero indeterminato di persone e quindi di ledere l'immagine dell'azienda.[36]

Ultimo caso che voglio analizzare è quello del controllo che si esaurisce con l'attestazione di inadempimento della prestazione. Ho scelto tre sentenze, diverse tra loro, ma che portano allo stesso risultato: l'affermazione della legittimità del controllo effettuato. La prima vicenda[37] è quella di una dipendente che utilizzava il telefono aziendale quale strumento di lavoro. Durante l'assenza per malattia il dispositivo viene lasciato in azienda. Dal momento che continuavano ad arrivare numerosi messaggi, il datore decide di controllarlo trovando, in primo luogo, scaricata l'applicazione di Facebook con la quale la dipendente intratteneva numerose conversazioni private durante l'orario di lavoro, scoprendo inoltre che la stessa aveva diffuso informazioni aziendali riservate a imprese concorrenti dirette. Il comportamento viene ritenuto costituente di grave illecito disciplinare e in grado di ledere gli obblighi di diligenza e fedeltà, contrattualmente assunti.

---

[33] La Corte in merito ricorda che: "il lavoratore, durante la malattia si deve adoperare affinché non venga ritardata la guarigione. Ciò comporta che debba astenersi da ogni attività, che possa compromettere la guarigione, non rilevando che ciò poi non sia accaduto."

[34] *Ex plurimis* Trib. Napoli, decreto n. 6655 del 25 febbraio 2015: un dipendente, assente per infortunio, posta delle foto che lo ritraggono alla Maldive e in locali notturni

[35] Cass. 13 ottobre 2021, n. 27939

[36] In questo senso si veda anche l'ordinanza 12 novembre 2018, n. 28878

[37] Tribunale di Bari, 10 giugno 2019, n. 2636. Si veda anche Corte di Appello di Roma, 22 marzo 2019, n. 1331

Nella seconda sentenza[38] un dipendente viene licenziato per i ripetuti accessi ai *social network* (16 al giorno durante tre ore di lavoro) tramite il *computer* aziendale. Il Tribunale di Brescia non ritiene invasione della *privacy* il controllo della cronologia del computer trattandosi di un uso improprio dello strumento di lavoro idoneo a incrinare la fiducia del datore e per questo motivo legittima il licenziamento.

L'ultima sentenza[39] è un caso che ha fatto parecchio discutere. Dopo che un dipendente, allontanandosi dalla pressa cui era addetto ne aveva provocato il blocco ed era stato sorpreso, nel mentre, al telefono, l'azienda decide di creare un falso profilo di donna in *Facebook* e di intrattenere una conversazione con il dipendente, accertando così che quest'ultimo usava i *social network* durante l'orario di lavoro. La Corte ritiene legittimo il licenziamento e afferma che la creazione del finto profilo non violi i principi di buona fede e correttezza dal momento che l'*account* era stato utilizzato come modalità di accertamento dell'illecito.

3.4 Il braccialetto elettronico alla prova dell'articolo 4

Passiamo ora a uno degli strumenti di controllo più innovativi e più contestati: il braccialetto elettronico. Questo strumento potrebbe essere in grado di rivoluzionare molti aspetti della vita umana spaziando dal tempo libero alla sanità e ancora all'ambito lavorativo. Il braccialetto elettronico fa parte dei cd *wearable devices* (letteralmente "dispositivi indossabili) e, grazie alla caratteristica di essere indossato, è in grado di lasciare all'utilizzatore entrambe le mani libere per svolgere le attività. Per quanto riguarda l'ambito lavorativo si può ben pensare che per un datore di lavoro potrebbe essere un bel vantaggio in termini di ottimizzazione della prestazione di lavoro dal momento che renderebbe più veloce e più precisa l'indicazione di ciò che ciascun dipendente dovrebbe fare in tempo reale. D'altro canto però il datore sarebbe in grado di immagazzinare un grande quantitativo di informazioni, sulla posizione e su ogni spostamento di chi lo indossa, potendo effettuare così un controllo continuo.

Nel 2016 Amazon ha brevettato *l'ultrasonic bracelet and receiver for detecting position* destinato a sostituire il lettore scanner utilizzato dai dipendenti. Il braccialetto in questione, lasciando le mani libere, è in grado di diminuire le tempistiche per portare a termine un singolo ordine. Lo strumento geolocalizza il dipendente, lo guida attraverso gli scaffali, comunica eventuali movimenti errati e fornisce un tempo massimo per spostarsi da una postazione all'altra. Se il dipendente supera il tempo ritenuto opportuno per portare a termine l'ordine, potrebbe essere soggetto ad una sanzione disciplinare.

[38] Tribunale di Brescia, 13 giugno 2016, n. 782
[39] Cass. civ. Sez. lav., 27 maggio 2015, n. 10955

Già a partire sempre dal 2016 anche Leroy Merlin aveva dotato i suoi dipendenti di un braccialetto elettronico, il *Gladiator*. Ciascun dipendente, all'inizio di ogni turno, doveva inserire la propria password nel dispositivo. Quest'ultimo emetteva un segnale acustico fino al momento in cui il lavoratore non si sarebbe messo in contatto con il cliente e, successivamente, partiva un conto alla rovescia di cinque minuti necessari per reperire la merce in magazzino e consegnarla al cliente. A differenza di Amazon, però, il tempo era solo indicativo e non veniva utilizzato a fini disciplinari. Ad aprile 2018, AVR S.p.A. (incaricata del servizio di pulizia delle strade del Comune di Livorno) aveva deciso di dotare i suoi dipendenti di un braccialetto in grado di attestare la vuotatura dei cestini e verificare che quest'ultimi fossero nella posizione corretta.
In tutti e tre questi casi la domanda che ci si pone è se i braccialetti debbano essere configurati come strumenti di controllo ovvero strumenti di lavoro. Come già evidenziato nel capitolo precedente non esiste una definizione precisa di strumenti di lavoro e per questo motivo la loro qualificazione è rimessa di volta in volta al datore di lavoro sulla base delle scelte organizzative. Così, per quanto riguarda il caso Amazon, i braccialetti, essendo dotati di un software che indica la posizione precisa della merce e che guida il lavoratore all'interno del magazzino, potrebbero essere ritenuti strumenti di lavoro in quanto indispensabili per svolgere l'attività. Lo stesso vale per il caso Leroy Merlin, in quanto il braccialetto sarebbe lo strumento con il quale il dipendente viene messo in contatto con il cliente. Diversa è invece la questione dei braccialetti per la vuotatura dei rifiuti in quanto lo strumento è definito indispensabile da un giudizio soggettivo del datore di lavoro (che afferma sia il modo più performante per accertare la vuotatura e la localizzazione dei cestini). Dal momento che il braccialetto potrebbe rientrare nella definizione di strumento di lavoro, il problema che si pone è sull'utilizzabilità delle informazioni raccolte. Sicuramente la prima condizione necessaria sarebbe che sia data al lavoratore adeguata informativa circa l'utilizzo di tale strumento e la seconda che sia rispettato quanto dettato dal codice della Privacy. Come esposto nel capitolo precedente il trattamento dovrebbe rispettare finalità legittime e determinate e i dati non potrebbero essere utilizzati per scopi diversi da quelli indicati *ab origine* ai lavoratori. Quindi un trattamento eseguito con uno scopo indeterminato non potrà mai essere ammesso. Il controllo continuo con finalità disciplinari che potrebbe scaturire dall'utilizzo del braccialetto elettronico non potrebbe mai portare a un trattamento lecito dei dati raccolti e inoltre sarebbe contrario al principio di "minimizzazione dei dati" di cui ho parlato nel capitolo precedente. Il principio di necessità, poi, non ammetterebbe che vengano raccolti dati diversi a quelli idonei a impartire direttive. Da questa analisi sarebbe difficile pensare che un tale strumento possa essere usato in conformità con le norme nazionali[40].

[40] In proposito Antonello Soro, presidente dell'Autorità Garante per la protezione dei Dati Personali, in un'intervista del 2 febbraio 2018 in cui si parlava del caso Amazon, alla domanda "C'è una violazione della normativa italiana in termini di privacy?" risponde: "Il sistema delle regole che disciplinano il trattamento dei dati personali e in particolare, in

Abbiamo visto come l'avanzamento della tecnologia ponga non pochi problemi per quanto riguarda la tutela della libertà e della dignità dei lavoratori messa a dura prova soprattutto dai più facili e più stressanti controlli che il datore di lavoro è in grado di eseguire. L'intreccio tra tecnologia e vita si fa sempre più stretto e si fa strada la necessità di adottare un ordinamento che tenga conto di tutti i nuovi rischi legati all'adozione di queste tecnologie.

questo caso, quello dei lavoratori deve rispondere a principi di proporzionalità, di trasparenza e di salvaguardia dell'attività dell'uomo che nell'ipotesi riferita non ci sarebbero quindi sarebbe in contrasto con le norme italiane…"

Conclusioni

Ripercorrendo l'analisi fin qui condotta, abbiamo visto come il vecchio articolo 4 dello Statuto non era stato in grado di tenere il passo dell'evoluzione tecnologica. Fino a che non è entrato in vigore il *Jobs Act*, la materia dei controlli a distanza era caratterizzata da un'ampia incertezza e la stessa giurisprudenza si muoveva con pareri discordi e talvolta in direzioni opposte a causa di una disciplina poco chiara e ormai obsoleta.

Abbiamo visto poi come il novellato articolo 4 abbia chiarito alcuni dei dubbi, come l'utilizzabilità dei dati a tutti i fini connessi al rapporto di lavoro, ma ne abbia posti altri, come la difficile categorizzazione degli strumenti in strumenti di lavoro o di controllo.

Infine abbiamo analizzato due delle numerose nuove tecnologie che entreranno sempre più a far parte delle organizzazioni e che stanno già mettendo in difficoltà la disciplina dei controlli a distanza.

Sicuramente il progresso tecnologico continuerà la sua avanzata e porterà, in ambito lavorativo, cambiamenti radicali. La disciplina riguardo i controlli dovrà inevitabilmente tenere conto delle nuove sfide lanciate dalle innovazioni tecnologiche bilanciando gli interessi opposti di lavoratori e datori di lavoro. Riguardo il futuro, non possiamo sapere con certezza quali cambiamenti avverranno, ma sicuramente avranno una portata tale da richiedere al legislatore una riflessione riguardo la materia.[41]

[41] Parole totali: 7007

Bibliografia

ALVINO I., L'articolo 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica. Diritto delle Relazioni Industriali, n. 4, 2014. pp. 999-1026

AVOGARO M., Abbandono ingiustificato del lavoro, GPS e investigatori privati tra controlli difensivi e Jobs Act. RIDL, 2016, II. p. 260

CRISCUOLO C., Controlli difensivi e codice della privacy. RIDL, 2017, II. pp. 39-44

CRISCUOLO C., Potere di controllo e computer aziendale. RIDL, 2019, II. pp. 9-15

DAGNINO E., Tecnologie e controlli a distanza. Diritto delle Relazioni Industriali, n. 4, 2015. pp. 988-1005

DEL PUNTA R., La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 51/2015). RIDL, 2016, I. pp. 96-109

DI MEO R., Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon. LLI, vol. 4, n. 1, 2018. pp. 11-18

GRAMANO E., La rinnovata (ed ingiustificata) vitalità della giurisprudenza in materia di controlli difensivi. Diritto delle Relazioni Industriali, n. 1, 2018. pp. 269-274

INGRAO A., Il braccialetto elettronico tra privacy e sicurezza del lavoratore. Diritto delle Relazioni Industriali, n. 3, 2019. pp. 895-916

INGRAO A., Il potere di controllo a distanza sull'ozio telematico e il limite del diritto alle *privacy* del lavoratore. RIDL, 2019, II. pp. 420-423

INGRAO A., Il controllo disciplinare e la privacy del lavoratore dopo il *Jobs Act*. RIDL, 2017, II. pp. 50-54

INGRAO A., Il controllo a distanza realizzato mediante Social network. LLI, vol. 2, n. I, 2016. pp. 106-118

MARESCA A., Controlli tecnologici e tutele del lavoratore nel *nuovo* art. 4 dello Statuto dei Lavoratori. RIDL, 2016, I. pp. 523-542

ROCCHINI E., Social network e controlli a distanza. Alla ricerca di un difficile equilibrio. Massimario di giurisprudenza del lavoro, n. 1, 2019. pp. 146-154

SALIMBENI M.T., La riforma dell'articolo 4 dello Statuto dei Lavoratori: l'ambigua risolutezza del legislatore. RIDL, 2015, I. pp. 589-616

TEBANO L., La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi? RIDL, 2016, I. pp. 347- 367

ZOLI C., Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma. RIDL, 2009, I. pp. 485-502

Fonte normative e prassi

Costituzione della Repubblica Italiana

L. 20 maggio 1970, n.300, c.d. Statuto dei Lavoratori

Dlgs. 4 marzo 2015, n. 151, c.d. Jobs Act

Dlgs. 30 giugno 2003, n. 196, c.d. Codice in materia di protezione dei dati personali

Regolamento (UE) n. 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, c.d. Regolamento generale sulla protezione dei dati

Gazzetta Ufficiale, n. 58, 10 marzo 2007, pubblicazione delle c.d. Linee guida del Garante per posta elettronica e internet

Relazione annuale 2010, Garante per la protezione dei dati personali (GPDP)

Giurisprudenza

Trib. Napoli, 25 febbraio 2015, n. 6655

Trib. Bergamo, 24 dicembre 2015

Trib. Brescia, 13 giugno 2016, n. 782

Trib. Bari, 10 giugno 2019, n. 2636

Corte di Appello di Roma, 22 marzo 2019, n.1331

Cass. 19 luglio 1985, n. 4271

Cass. 25 gennaio 1992, n. 829

Cass. 3 aprile 2002, n. 4746

Cass. 17 luglio 2007, n. 15892

Cass., Sez. L., 2010, n. 4375

Cass. 23 febbraio 2012, n. 2722

Cass. 4 aprile 2012, n. 5371

Cass. 18 aprile 2012, n. 16622

Cass. Civ. Sez. Lav., 27 maggio 2015, n. 10955

Cass., Sez. L., 2016, n. 9904

Cass. 13 marzo 2018, n. 6047

Cass. 27 aprile 2018, n. 10280

Cass. 13 ottobre 2021, n. 27939