UNIVERSITÀ DI PISA

Dipartimento di Economia e Management

Corso di Laurea Magistrale in

Consulenza Professionale alle Aziende

Tesi di Laurea

IL CONTROLLO DEI LAVORATORI DOPO IL JOBS ACT

Relatore:

Prof. ssa Giuseppina MORTILLARO

Candidato:

Lorenzo ROGAI

ANNO ACCADEMICO 2015 -2016

INDICE

INTRODUZIONE

Il Jobs Act ha avuto come scopo quello di rivedere aggiornare e modernizzare la normativa sul lavoro. Infatti ha razionalizzato i contratti di lavoro iniziando a svuotare il bacino delle collaborazioni “grigie” a favore del contratto subordinato. Ha creato una maggiore flessibilità in uscita con una nuova e razionale disciplina dei licenziamenti ha inoltre modificato gli ammortizzatori sociali (CIG e disoccupazione) ed ha previsto il potenziamento degli istituti per la conciliazione vita-lavoro ed anche una maggiore flessibilità del rapporto di lavoro. In una così estesa riforma non poteva mancare un miglioramento ed un aggiornamento della disciplina dei controlli, che il datore di lavoro può effettuare sul lavoratore, che tenesse conto dell’evoluzione sia tecnologica sia sociale sia giurisprudenziale.

In questa tesi andremo quindi ad analizzare il nuovo art. 4 dello statuto dei lavoratori cosi come modificato con il D.lgs. 151/2015. Per vedere al meglio quali sono state le modifiche apportate considereremo innanzitutto il percorso storico, partendo dalla nascita dell’art. 4 della L. 300/1970, considerando quali furono i fini che portarono il Legislatore a scrivere l’art. 4. Di conseguenza metteremo in evidenza i limiti che aveva il vecchio art. 4 che, per il periodo storico in cui era stato scritto e le modalità di lavoro del momento, non andava a considerare determinate problematiche. Vedremo poi che queste lacune normative hanno portato alla creazione del filone giurisprudenziale dei c.d. “controlli difensivi” discussi e apprezzati da parte della dottrina. Con il prosieguo dell’analisi vedremo anche quali sono le novità portate dall’aggiornamento normativo nel dettaglio e se queste novità vanno effettivamente ad equilibrare il rapporto tra datore di lavoro e lavoratori in materia di controllo. Una delle novità più interessanti e che più vanno a impattare sulla normativa è l’espresso richiamo al Codice della Privacy che va a tutelare i dati del lavoratore e pone nuove restrizioni che in passato non erano considerate. Infatti nonostante la norma

ponga una moderna apertura sulle modalità di controllo, soprattutto in merito agli strumenti di lavoro per i quali non è richiesto l'accordo sindacale, il Garante della privacy, a tutela del diritto costituzionale, vincola il datore di lavoro a rispettare le disposizioni in materia di privacy che, se non applicate, renderebbero sanzionabile anche penalmente il controllo del datore di lavoro evidentemente effettuato senza ottemperare alle disposizioni del Garante. Analizzeremo quindi nel dettaglio, in riferimento a determinati strumenti di lavoro, come la nuova normativa va ad impattare nel concreto.

1.ISTITUZIONE E STORIA DEI CONTROLLI PREVISTI DALLO STATUTO DEI LAVORATORI

In questo capitolo percorreremo la storia dell'art. 4 dello statuto dei lavoratori, ricordando le finalità che portarono all'istituzione dell'articolo e i problemi pratici che le aziende si sono trovate ad affrontare per il progresso tecnologico andando a creare situazioni problematiche che il Legislatore del 1970 non aveva considerato. Vedremo quindi quali sono state le cause che hanno portato al filone giurisprudenziale dei c.d. "controlli difensivi" e cercheremo così di fornire le ragioni che hanno portato alla modifica del predetto art. 4.

1.1 Il contesto tecnologico e le finalità considerate nel 1970

Il potere di controllo sui lavoratori è da sempre ritenuto una componente naturale del potere direttivo. È estremamente inerente alla posizione dell'imprenditore in quanto "capo" dell'impresa (art.2086 c.c.), essendo finalizzato a garantire la corretta e tempestiva esecuzione degli obblighi lavorativi, nonché, l'osservanza delle regole che disciplinano la condotta del lavoratore all'interno dell'impresa. Lo statuto dei lavoratori si è preoccupato anche di limitare le modalità di esercizio dei controlli. Le norme relative al controllo sono al Titolo I dello Statuto, l'art.2 limita l'uso delle guardie giurate, disponendo le modalità e gli scopi per cui il datore di lavoro può usufruirne. L'art.3 dedicato al personale di vigilanza, ha lo scopo di prevenire i controlli occulti, sul presupposto che questi siano lesivi per la dignità del lavoratore. Tuttavia a fronte di questa esigenza vi è però quella dell'azienda a prevenire e/o verificare la commissione di illeciti, ad esempio in quelle attività che registrano spesso furti ed irregolarità di vario genere da parte dei dipendenti. L'art 6, proibisce le visite personali di controllo sul lavoratore, a meno che non siano indispensabili ai fini della tutela del patrimonio aziendale, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti. Infine l'art.8 dello Statuto dei Lavoratori si è preoccupato anche dell'aspetto della vita privata del lavoratore. Infatti "è fatto divieto al datore di lavoro, ai fini dell'assunzione come nel corso dello

svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore". [1]

In questo lavoro ci occuperemo dell'art. 4 che tratta la materia dei controlli a distanza. La norma in oggetto emanata nel 1970 aveva lo scopo di andare a tutelare la dignità personale del lavoratore, evitando che il datore di lavoro fosse libero di effettuare controlli a distanza senza alcuna limitazione. Poiché si trattava di tutelare diritti fondamentali della persona, il mancato rispetto delle disposizioni dell'art. 4 comportava per il datore di lavoro sanzioni sia di tipo amministrativo che penale ai sensi dell'art.38 dello Statuto dei lavoratori. Quest'articolo è stato modificato con il D.lgs. 151/2015 Jobs Act ed analizzeremo a fondo, in questa tesi, quali sono state le novità.

Per capire al meglio ciò che ha spinto il Legislatore a modificare la norma è importante partire dall'articolo prima della modifica. Intanto riportiamo il nuovo testo dell'art. 4 mettendolo a confronto con il testo prima della riforma:

Testo in vigore	**Testo precedente**
Art. 4 - Impianti audiovisivi e altri strumenti di controllo	**Art. 4 - Impianti audiovisivi**
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	**1.** È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. **2.** Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la

[1] R. Del Punta, *Diritto del Lavoro,* VII Giuffrè Editore, Milano 2015, pp.505-512

Testo in vigore	Testo precedente
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.	commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti. **3.** Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente L., dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti. **4.** Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

L'art. 4 della L. 300/70 (più avanti citata come S.L ovvero Statuto dei lavoratori) regolamentava il controllo a distanza dei lavoratori ponendone il divieto. Il termine "controllo a distanza" ha un significato sia spaziale ovvero di tipo geografico sia temporale in quanto differito nel tempo. In pratica è proibito controllare il lavoratore direttamente e in contemporanea con l'utilizzo di monitor e a posteriori, come nel caso di immagini videoregistrate. Questo controllo non può avere ad oggetto l'attività lavorativa e ogni altra attività svolta in azienda come le pause e gli spostamenti.[2] Quest'articolo venne istituito con la

[2] R. Schiavone, *Controllo dei Lavoratori*, Milano, Gruppo 24ore, 2015, P. 86

finalità di regolare le installazioni di strumenti che non erano richiesti dalla prestazione lavorativa ma che potevano essere utilizzati per controllare i lavoratori.

Il Legislatore intendeva regolare una realtà produttiva da cui poteva derivare una possibile attività di controllo. La norma aveva ad oggetto quegli strumenti che ad esempio consentivano di controllare la continuità di funzionamento di un macchinario, di rilevare la quantità di energia elettrica consumata, di registrare le conversazioni che di fatto consentivano di assumere informazioni sulla quantità di ore lavorate che permettevano quindi di ricostruire a distanza l'attività svolta dal lavoratore.

In quel periodo storico, ovvero gli anni 70, dove il computer, gli smartphone e i tablet erano ben lontani da entrare nella quotidianità delle aziende, il Legislatore voleva limitare l'impiego delle apparecchiature che non rientravano fra gli "strumenti di lavoro" e che quindi non erano necessarie all'adempimento dell'obbligazione lavorativa stipulata.

Il Legislatore, per ovviare a queste problematiche, inserì il divieto assoluto di impiego di strumenti la cui finalità fosse quella del controllo dell'attività lavorativa, ammettendo l'installazione di apparecchiature solo per finalità organizzative o di sicurezza sul lavoro. L'installazione di queste apparecchiature poteva essere consentita solo a seguito di un accordo con il sindacato oppure mediante autorizzazione rilasciata dalla DTL competente. Il mancato accordo o la mancata autorizzazione non consentiva di fatto l'utilizzo di queste apparecchiature. Il presupposto della norma è quello di non spingere l'attività di vigilanza oltre limiti tali da escludere qualsiasi spazio di autonomia e riservatezza.[3]

[3] L. D'andrea E. Morriconi, *Controlli a Distanza: La Disciplina Prima e Dopo la Riforma*, Milano, Ipsoa, 2016, p.2

Le maggiori difficoltà interpretative sono cominciate ad emergere con il progresso tecnologico che portava nuovi strumenti all'interno delle aziende che, per i componenti o i software che venivano utilizzati dalle aziende produttrici, consentivano nuove modalità di controllo a distanza. Questo ha fatto nascere nuovi interrogativi come, ad esempio, se fosse necessario l'accordo con i sindacati o l'autorizzazione della DTL anche per l'utilizzo da parte del lavoratore di questi strumenti. Tuttavia in una realtà sempre più veloce e frenetica delle attività lavorative non si poteva immaginare un quadro in cui dovesse essere richiesta un'autorizzazione o raggiunto un accordo per fornire al lavoratore gli strumenti utili a svolgere la propria prestazione, l'eventuale accordo sarebbe stato un ostacolo che poteva mettere in crisi l'azienda.[4]

Di fronte a questa difficoltà parte della dottrina aveva ritenuto di escludere gli strumenti di lavoro dall'area di applicazione dell'articolo sostenendo che per gli stessi non fosse necessaria la preventiva autorizzazione o il preventivo accordo. La dottrina riteneva che si dovesse distinguere da un lato l'installazione dell'apparecchiatura da cui può derivare il controllo dell'attività lavorativa e dall'altro quello della possibilità di andare a controllare lo strumento di lavoro per estrapolare le informazioni riguardanti lo svolgimento della mansione. Al comma 2 il vecchio articolo tuttavia inseriva un'apertura al divieto consentendolo nei casi in cui ci fossero esigenze di tipo organizzativo produttivo ovvero di sicurezza sul lavoro. In questo caso, quand'anche ne derivasse una possibilità di controllo a distanza dell'attività del lavoratore, veniva ritenuta lecita in quanto si definiva come controllo "preterintenzionale". Questo concetto andava a consentire il controllo del lavoratore nel caso in cui il datore di lavoro controlla il lavoratore senza averne l'intenzione in quanto installate le telecamere

[4] I. Alvino, "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", *Labour & Law Issues*, 2, n.1, (2016): pp. 4-5.

senza avere quello specifico scopo, ma uno degli scopi legittimati dal secondo comma. È evidente che per andare a verificare la bontà delle intenzioni del lavoratore occorreva una disamina sull'elemento soggettivo del datore di lavoro. Ma di una tale indagine non si è mai materializzata neppure l'ombra nelle aule giudiziarie in quanto non avrebbe senso. Di fatto quindi l'implicazione della norma era un'altra ovvero l'installazione doveva essere consentita da un "giustificato motivo" che infatti prevedeva una procedura autorizzativa. La norma andava a regolare le condizioni affinché si potesse installare lo strumento ma non diceva niente in merito alla possibilità del datore di lavoro di interrogare le informazioni eventualmente raccolte. Quindi questo problema era di grosso rilievo e sul punto, ovvero della possibilità di utilizzare le informazioni o meno, la dottrina era divisa. Infatti si può dare un'interpretazione, che da Del Punta viene definita "Radicale" o "Ipocrita". Radicale ovvero vietare in ogni caso l'utilizzo delle informazioni eventualmente raccolte in ragione del divieto assoluto posto al primo comma della norma. Ipocrita nel senso che non veniva affrontato il problema dalla norma, che era tutt'altro che secondario, e di conseguenza utilizzabili. Secondo Del Punta l'interpretazione più corretta sarebbe stata quella radicale in ragione del primo comma della norma. Tuttavia al contempo pensare che il datore di lavoro che avesse sorpreso il lavoratore a compiere un illecito potesse fingere di non averlo visto e rinunciare a perseguirlo sul piano disciplinare è altrettanto illogico.[5]

Questo ha fatto sì che, nei casi in cui ci fosse stato l'accordo per avere l'autorizzazione all'installazione delle apparecchiature, i limiti venissero definiti all'interno dei CCNL dove venivano stabiliti anche le modalità di utilizzo dell'informazioni raccolte di cui chiaramente, spesso, veniva vietato l'utilizzo. Inoltre l'azienda veniva messa "con le spalle al muro" anche dall'autorizzazione

[5] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro, 2015* p.4

della DTL la quale, nel provvedimento autorizzatorio, vietava l'utilizzo delle informazioni per fini disciplinari. Sicuramente questa è stata una delle ragioni che hanno portato le aziende a non trovare un accordo sindacale o richiedere l'autorizzazione alla DTL per non vedersi del tutto rimossa la possibilità di utilizzare le informazioni raccolte nel caso in cui ce ne fosse stata la necessità.

1.2 Le problematiche derivanti dal progresso tecnologico.

Un altro problema che ha messo in evidenza i limiti dell'art. 4 S.L. è rappresentato dal fatto che i nuovi strumenti tecnologici, che siano o meno strumenti di lavoro, consentono di ottenere informazioni incrociando i dati dei vari dispositivi dati in uso al lavoratore, basti pensare a quanti strumenti tecnologici hanno al loro interno il GPS che consente di rilevare la posizione esatta in cui si trova lo strumento tecnologico. Per rendere ancora più chiara la problematica in esame poniamo in rilievo il seguente esempio: pensiamo ad un computer dell'ufficio dato in uso al lavoratore per svolgere la sua attività lavorativa sia stato infettato da un virus informatico; la rimozione potrebbe comportare la verifica dei siti navigati dal lavoratore per individuare la causa del problema o comunque le operazioni eseguite su internet in un determinato lasso temporale. Oppure un altro esempio potrebbe essere la verifica delle mail inviate da parte del lavoratore ai clienti per accertarsi della chiusura di un contratto di fornitura. Le moderne tecnologie portano quindi a prendere in considerazione nuove problematiche e nuove esigenze che portano a dover definire i limiti entro cui il datore di lavoro può muoversi. È evidente che il principio della necessaria autorizzazione è in molti casi inadeguato, tuttavia allo stesso tempo il monitoraggio degli strumenti deve essere limitato ma non vietato alla radice.[6] Questo aspetto ha portato alla nascita del filone giurisprudenziale dei controlli difensivi che andremo ad analizzare nel successivo paragrafo.

[6] Cfr, I. Alvino, Labour & Law Issues, *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*, Op cit. pp. 6-8.

Un'altra problematica di grande importanza che ha fatto emergere ulteriori limiti della disposizione è quello relativo ai diritti del lavoratore di cui deve essere garantita la protezione nel caso dei controlli a distanza.

Sotto questo punto di vista si è soliti affermare che l'art. 4 S.L. detta le regole volte a garantire la protezione della dignità e della riservatezza del lavoratore. Parte della dottrina ha ritenuto che l'art. 4 avesse anticipato la successiva L. n. 675 del 31 dicembre 1996 in merito di tutela delle informazioni personali. Il bene della privatezza delle informazioni con il passare del tempo ha avuto un'interpretazione molto più ampia rispetto a quella pensata dal Legislatore degli anni 70 il quale voleva tutelare il lavoratore da situazioni di stress lavorativo dovuto a un controllo continuo sulla sua prestazione. Infatti già il fatto che l'art. 4 sia stato inserito nel titolo I dedicato alla "libertà e dignità del lavoratore" rende chiara la volontà di voler tutelare tale diritto.

Tuttavia il progresso tecnologico ha portato a ridurre la protezione del lavoratore in merito alle informazioni sensibili ottenibili del lavoratore, inoltre tale aspetto non era affatto tutelato nella norma originaria. Anche con l'emanazione del D.lgs. 196/2003, il Codice della Privacy, non vi sono stati cambiamenti. Infatti fra i due impianti normativi c'è stato più un "patto di non belligeranza" che uno sviluppo di interazioni. Eventuali interazioni vennero successivamente sviluppate dalla giurisprudenza e dal Garante; quasi come se le norme di tale codice fossero di competenza del solo Garante.[7] I nuovi strumenti di lavoro possono infatti carpire informazioni profondamente personali del lavoratore solo, ad esempio, dalla verifica dei siti visitati dal lavoratore si può capire l'orientamento sessuale politico e religioso. Cerchiamo di rendere più chiara l'affermazione appena fatta con un esempio: riprendiamo il caso del virus del computer, dall'analisi della cronologia dei siti visitati si potrebbe evincere l'orientamento sessuale e politico

[7] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, Op cit., p.9

del lavoratore. Questo porta a dover tutelare da una parte l'interesse del datore di lavoro ad accertarsi che il lavoratore non navighi, durante l'orario di lavoro, su siti non rilevanti ai fini della prestazione e dall'altra la riservatezza delle informazioni personali del lavoratore. Infatti l'accesso alle informazioni riservate potrebbe essere una conseguenza dell'attività di controllo. [8]

1.3 Il filone giurisprudenziale dei "controlli difensivi"

Nella sua stesura originaria prima della riforma del Jobs Act sanciva: "è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori". Quest'impostazione segue la linea assunta dal Legislatore ed assicura una tutela piena, spesso anche esagerata, del lavoratore. Questa norma nasce con l'obiettivo di andare a tutelare la "dignità personale" del lavoratore. [9] L'art 4 S.L. per come era impostato consentiva l'utilizzo di impianti audiovisivi di controllo a distanza soltanto per finalità di tipo organizzativo produttive, per la sicurezza dei lavoratori ma non per la tutela del patrimonio aziendale. In ogni caso l'installazione era consentita solo previo accordo fra l'azienda e i rappresentanti del sindacato dei lavoratori o, in assenza di quest'ultimo, con autorizzazione della DTL. L'installazione delle telecamere non poteva essere in ogni caso finalizzata al controllo del lavoratore. Nell'ipotesi in cui avesse telecamere o altri strumenti per il controllo a distanza senza l'accordo sindacale o l'autorizzazione della DTL le informazioni ottenute sarebbero state inutilizzabili. La giurisprudenza posta di fronte a casi concreti nei quali il datore di lavoro aveva utilizzato le informazioni acquisite tramite controlli a distanza, in specie a mezzo di strumenti informatici, come base dell'adozione di provvedimenti disciplinari ha tracciato nuovi meccanismi interpretativi che sono andati a dirimere controversie in tema di illegittimi

[8] I. Alvino, Labour & Law Issues, *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*, Op Cit. pp. 10-11.
[9] M.T. Carinci, Labour & Law Issues, *Il controllo a distanza dei lavoratori dopo il "jobs act": spunti per un dibattito*, Università degli studi di Milano, 2016, p.3

licenziamenti e illegittimo esercizio del potere disciplinare basato sull'utilizzabilità dei dati raccolti tramite i controlli. È evidente che l'art. 4 aveva un enorme vuoto in quanto non era ben chiaro quali mezzi tecnologici potessero rientrarvi e quali no. Infatti l'irrompere delle nuove tecnologie ha modificato l'ambiente di lavoro superando così la distinzione tra strumento di lavoro e strumento di controllo. Basti pensare ai computer, ai tablet, agli smartphone che fanno parte dell'attuale contesto produttivo ma che consentono, anche in vari modi, di controllare il lavoratore. Di conseguenza una domanda che ci si pone è se questi strumenti di lavoro dovessero essere oggetto di autorizzazione da parte della DTL o del sindacato dei lavoratori. Tuttavia è chiaro ed evidente che ai giorni nostri nessuno potrebbe interfacciarsi col mercato privandosi di questi strumenti tecnologici.

L'avvento delle nuove tecnologie ha di fatto spiazzato l'art. 4 e il suo mancato coordinamento con il Codice della Privacy ha di fatto posto gravi problemi. Infatti l'art 4 incentrava il proprio intervento sul controllo dei lavoratori mentre il codice della privacy sul trattamento dei dati personali.[10]

Le problematiche sopra elencate hanno portato al formarsi di un massiccio contenzioso, che poneva nuovi interrogativi e questioni che portarono la giurisprudenza a legittimare l'utilizzo dei controlli anche senza il previo accordo sindacale o amministrativo. Gran parte dei giudici ritenevano che l'interesse del datore di lavoro di preservare il patrimonio aziendale fosse meritevole di tutela e che lo stesso potesse essere soddisfatto impiegando strumenti di controllo la cui installazione non doveva essere soggetta ai limiti prescritti dall'art. 4. La giurisprudenza affermava che il controllo era lecito se qualificabile come "difensivo" ovvero giustificato dall'interesse del datore di lavoro a difendersi dalla commissione di illeciti da parte del lavoratore. Questo approccio era

[10] M.T. Carinci, Labour & Law Issues, *Il controllo a distanza dei lavoratori dopo il "jobs act": spunti per un dibattito*, Op Cit. pp. 5-6.

tuttavia paradossale, in quanto un controllo era ritenuto legittimo sulla base di un dato *ex post.* Ciò a maggior ragione in quanto ad essere illecita anche penalmente, *ex ante,* era l'installazione di strumenti che rendevano possibile il controllo. In pratica la legittimazione dei controlli difensivi implicava, in definitiva, "lasciare libero il datore di lavoro di svolgere controlli occulti in ogni caso: se infatti, dopo l'esercizio del potere, non risulteranno commessi (gravi) inadempimenti/illeciti, i controlli rimarranno presumibilmente ignoti e non puniti; se, invece, emergeranno delle mancanze o illeciti, le prove di essi potranno essere adoperate contro il lavoratore, perché saranno proprio queste ultime a giustificare, a posteriori appunto, il controllo occulto".[11] Un' importante sentenza della Suprema Corte la n. 4746 del 3 aprile 2002 affermò la totale esclusione dall'ambito di applicazione dell'art. 4 S.L., delle forme di controllo dirette ad accertare condotte illecite del lavoratore. Con questa sentenza la cassazione operava una distinzione sulla finalità dei controlli ovvero quelli derivanti da esigenze organizzative e produttive e di sicurezza del lavoro e quelli volti ad accertare condotte illecite dei lavoratori. Quest'ultimi, in quanto non contemplati dalla norma, erano ritenuti sempre consentiti. [12] Con questa pronuncia la corte andava a consentire l'utilizzo delle informazioni cosi raccolte per fini disciplinari. La falla interpretativa tuttavia stava nel fatto che, erano condotte illecite poste in essere sul posto di lavoro quindi individuabili a seguito di un'attività di controllo.

La giurisprudenza andò così a definire questi controlli come "quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti non riguardino l'esatto adempimento delle obbligazioni

[11] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, Op cit., p.5
[12] Cfr I. Alvino, Labour & Law Issues, *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*, Op cit. pp. 11-13.

discendenti dal rapporto, bensì la tutela di beni estranei al rapporto stesso"[13]. Inoltre il dipendente, controllato in questo modo, deve aver già commesso o comunque devono sussistere fondati sospetti del compimento di un atto illecito che mini il patrimonio aziendale. La questione quindi si sposta oltre che sul controllo in sé anche sull'utilizzabilità dei dati così raccolti. Ai fini di poter classificare o meno il controllo come difensivo la valutazione non potrà che essere fatta ex post.

La corte di cassazione successivamente corresse la tendenza della precedente sentenza, con la n.15892 del 17 luglio 2007. La sentenza verteva su un *badge* utilizzato per l'accesso ad un garage aziendale. In merito a questo ha affermato che la possibilità di utilizzare le informazioni risultanti da tale strumento era condizionata al previo accordo o autorizzazione che nel caso difettava. Ma mentre asseriva questo contrapponendosi cosi alla sentenza del 2002, ha aggiunto due affermazioni significative.

La prima è che restavano esclusi dal perimetro dell'art. 4 i controlli difensivi finalizzati alla tutela di "beni estranei al rapporto di lavoro" non ben specificati. La seconda affermazione riportava all'interno dei controlli dell'art. 4 i controlli rivolti all'accertamento di un inadempimento contrattuale. Sembrava quasi che la corte non si fosse accorta di stare ammettendo l'utilizzo di informazioni per vagliare provvedimenti disciplinari a seguito di controlli a distanza purché ci fosse stata l'autorizzazione all'installazione dello strumento. Successivamente la sentenza n.4375 del 23 febbraio 2010 dette continuità alla sentenza del 2007. Aveva infatti ritenuto inutilizzabile, per difetto di autorizzazione, le informazioni relative a inadempimenti del lavoratore, consistiti in ingiustificati accessi ad internet durante l'orario di lavoro, che erano stati registrati dal programma Super Scout. Si staccò da questa posizione la sentenza n. 16622 del 1 Ottobre 2012, in

[13] Cit Cass. civ., sez. lav., 23 febbraio 2012, n. 2722

merito a un controllo effettuato tramite un altro sistema informatico, preferì il seguente principio di diritto: "il divieto di controlli a distanza *ex* art. 4, della L 300/1970, implica, dunque, che i controlli difensivi posti in essere con il sistema informatico Blues 2002, ricadono nell'ambito della L. 300/1970, art. 4 comma 2, e , fermo il rispetto delle garanzie procedurali previste, non possono impingere la sfera della prestazione lavorativa dei singoli lavoratori; qualora interferenze con quest'ultima vi siano, e non siano stati adottati dal datore di lavoro sistemi di filtraggio delle telefonate per non consentire, in ragione della previsione dell'art. 4, comma 1, di risalire all'identità del lavoratore, i relativi dati non possono essere utilizzati per provare l'inadempimento contrattuale del lavoratore medesimo".[14]

I controlli difensivi possono essere in sostanza:

- Controlli difensivi preventivi
- Controlli difensivi successivi

I controlli difensivi preventivi sono quei controlli che vengono posti in essere dal datore di lavoro, nei casi in cui l'illecito si sia già verificato da parte del lavoratore e di conseguenza sono effettuati al fine di evitare che l'illecito possa ripetersi. Infatti la finalità è quella della prevenzione.

I controlli difensivi successivi si differenziano da quelli preventivi in quanto il datore di lavoro ha già dei sospetti qualificati ovvero gravi, precisi, e concordanti nei confronti di uno specifico lavoratore ed il controllo ha finalità di verificare quello specifico lavoratore per reprimere il suo comportamento illecito.

Vi sono poi i controlli così detti "*controlli occulti*" ovvero predisposti all'insaputa dei lavoratori tramite sistemi tecnologici oppure tramite altro personale. Anche questa è oramai una procedura tendenzialmente ammessa in

[14] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro,* Op cit., p.7

quando prende origine dalle stesse argomentazioni che legittimano i controlli difensivi.

Una recente sentenza della cassazione n. 10955/2015[15], li ammette "in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa restando comunque necessario che le attività di accertamento si esplichino con modalità che contemperino l'interesse del datore al controllo e alla difesa dell'organizzazione con il rispetto delle garanzie di liberà e dignità dei dipendenti, ed in ogni caso rispettino i canoni generali della correttezza e buona fede contrattuale"[16]. Nella fattispecie era stato ritenuto lecito la creazione di un account fittizio su facebook al fine di verificare la presenza sul social network da parte del lavoratore durante l'orario di lavoro. Venne considerato lecito in quanto non aveva ad oggetto il controllo dell'attività lavorativa ma bensì il perpetrare di comportamenti illeciti già manifestati da parte del dipendente. La pronuncia ha adottato un'accezione ampia di controllo difensivo esentato dall'art. 4, vale a dire quello "destinato a riscontrare e sanzionare un comportamento idoneo a ledere il patrimonio aziendale, sotto il profilo del regolare funzionamento e della sicurezza degli impianti". Dove tramite il riferimento alla tutela del patrimonio, si è recuperato il controllo su meri inadempimenti contrattuali[17]. Questo tipo di controllo non venne fatto rientrare nella disciplina dell'art. 4 con conseguente ammissibilità del controllo cosi effettuato. Gran parte della dottrina sostiene infatti che se ad essere oggetto del controllo è l'attività illecita posta in essere in ottemperanza dell'attività lavorativa allora si rientra nella disciplina dell'art. 4 dello statuto dei lavoratori, se si tratta invece di una attività illecita, ma che non è significativa quanto alla valutazione della prestazione lavorativa svolta allora tale articolo non trova

[15] V. Cass., 27 maggio 2015, n.10955, FI, 2015, I, 2316.
[16] Cfr L. D'Andrea E. Morriconi, *Controlli a Distanza: La Disciplina Prima e Dopo la Riforma*, Op cit. pp. 6-8
[17] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, Op cit., p.8

applicazione. Quindi nel concreto bilanciamento degli interessi in gioco prevale la tutela del patrimonio e dell'immagine aziendale rispetto alla dignità del lavoratore.

Un'altra sentenza interessante che si è occupata della materia è la n. 5599/1990 della cassazione in cui venne legittimato il controllo occulto anche svolto di notte e clandestinamente purché svolto dal datore di lavoro o da un suo preposto in quanto soggetti ben noti al lavoratore. A fronte di questa possibilità concessa al datore di lavoro resta fermo in ogni caso il divieto di ricostruire l'attività e la prestazione del prestatore anche tramite apparecchiature software come ad esempio lettura e registrazione sistematica della messaggistica e-mail, memorizzazione delle pagine web visitate dal lavoratore, lettura e registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo. In tal senso ad intervenire è stato il garante della privacy attraverso la delibera n. 13 del 1° marzo 2007.

Infatti è ben noto che in questo delicato argomento dei controlli spesso ci si trova a confrontarsi oltre che con l'art. 4 dello statuto dei lavoratori anche con la normativa relativa alla protezione dei dati personali.[18]

[18] L.D'andrea E. Morriconi, *Controlli a Distanza: La Disciplina Prima e Dopo la Riforma*, Op Cit. p. 9.

2.LE NOVITÀ APPORTATE DALLA RIFORMA DEL LAVORO.

Nel capitolo 2 vediamo nel dettaglio quali sono state le modifiche apportate dalla riforma dell'art. 4. Esamineremo le problematiche inerenti gli "strumenti di lavoro" ovvero ciò che la norma vuole far rientrare tra gli strumenti di lavoro e ciò che non vuol far rientrare. Porremo un primo accenno sul ruolo che va a coprire il codice della privacy e le relative problematiche applicative. Concluderemo con un breve accenno al regime transitorio, in riferimento alle domande che potrebbero porsi le aziende e concluderemo il capitolo fornendo un accenno alle novità che potranno esserci in merito alla contrattazione di prossimità.

2.1 Le modifiche apportate al vecchio art. 4

Il nuovo art. 4, Stat. lav.
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

Il nuovo art. 4, Stat. lav.
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***.

La prima modifica che si nota è la variazione del termine “apparecchiatura” con il termine “strumento” apre a migliori interpretazioni che lo rendono adattabile anche ai nuovi progressi tecnologici.

La seconda modifica, ben più rilevante, è l’eliminazione del termine “divieto assoluto di utilizzo” di strumenti di controllo a distanza imposto dal vecchio primo comma dell’art. 4 dello statuto dei lavoratori. Questo è stato sostituito rendendo non più un’eccezione l’utilizzo di telecamere in caso di necessità organizzative o di tutela del patrimonio aziendale, bensì regola positiva. La norma come posta in precedenza, ovvero l’eccezione all’utilizzo delle telecamere in caso di tutela del patrimonio aziendale, aveva portato a quel filone giurisprudenziale che vedeva appunto la tutela del patrimonio aziendale come una deroga all’art. 4 e quindi alla richiesta dell’autorizzazione all’installazione

delle telecamere. Per come adesso è posta la norma, la tutela del patrimonio aziendale diventa un fine per poter stipulare l'accordo sindacale o richiedere l'autorizzazione alla DTL per poter richiedere l'autorizzazione all'installazione delle telecamere.

Si va quindi a inquadrare una rinnovata ratio, contenente una disciplina positiva delle ipotesi e delle modalità in cui l'utilizzo di detti strumenti è lecito e non più un espresso divieto seppur flessibilizzato. Questa nuova ratio secondo qualche dottrina va a eliminare il vecchio principio cardine dell'art. 4 relativo alla dignità del lavoratore dipendente. Si ritiene: "affermare che una certa attività è vietata e disciplinare poi i casi in cui a tale divieto è consentito derogare non è lo stesso che limitarsi a disciplinare (regolandoli) i casi in cui tale attività è consentita. (*Omissis*). Non è una differenza di poco conto, quantomeno ove si voglia privilegiare una valutazione sistematica della materia" [19]. Può quindi ora configurarsi la fattispecie per cui il controllo a distanza sia una logica conseguenza di efficentamento aziendale e quindi in ogni caso consentita? Sicuramente no in quanto la giurisprudenza, (V. sentenza n.15892 del 17 luglio 2007) parla di "insopprimibile esigenza di evitare condotte illecite, la quale non può giustificare un sostanziale annullamento di ogni forma di garanzia di dignità e riservatezza".

Altra novità è la separazione del concetto di impiego e installazione. Infatti nel vecchio articolo venivano posti da un punto di vista interpretativo sullo stesso piano. Nella vecchia formulazione al primo comma si parlava di divieto d'uso e al secondo invece a seguito dell'accordo sindacale di installazione per poi parlare di modalità d'uso in relazione all'autorizzazione della DTL.

[19] L.A. Cosattini, *Le modifiche all'art. 4, Stat. lav. sui controlli a distanza, tanto rumore; per nulla?* In *Il lavoro nella giurisprudenza*, n. 11/2015, p. 986.

Nel riscritto art. 4 la scissione tra impiego e installazione è espressa lessicalmente e per come è scritta fa evincere che solo a seguito del lecito impiego e quindi solo nei casi in cui i fini siano leciti (esigenze organizzative e produttive) ne è concessa l'installazione. Quest'impostazione può portare a due possibili chiavi interpretative della norma:

1. Si potrebbe affermare che la disposizione è chiara e precisa nel subordinare al previo accordo sindacale l'installazione. Di conseguenza nel caso in cui il datore di lavoro installasse le telecamere senza accordo sindacale si configurerebbe un illecito, mentre per come era posta in precedenza la norma l'installazione delle telecamere avrebbe configurato un reato di pericolo. Quindi la norma così posta sembrerebbe andare in senso peggiorativo dal punto di vista del datore di lavoro e in senso migliorativo nei confronti del lavoratore che si vedrebbe maggiormente tutelato. Quindi il datore di lavoro, anche nel caso in cui l'impiego fosse consentito non potrebbe installare le telecamere e successivamente chiedere l'autorizzazione, perché l'assenza dell'autorizzazione comporta di per sé la violazione della norma. Certo è che la modifica dell'art. 4 e quindi la finalità del Legislatore è quella di andare ad agevolare i controlli e non a limitarli ulteriormente, inoltre è importante considerare che i sindacati non sarebbero, anche in caso di urgenza come ad esempio per la sicurezza dei lavoratori, celeri nel rilasciare l'autorizzazione[20].
2. La seconda impostazione che è quella da preferire alla luce delle considerazioni fatte nel punto precedente vede un'interpretazione estensiva del termine impiegare, inteso nell'ampio senso di "adoperare per una certa finalità" andando così a ricomprendere al suo interno anche la fase di installazione che presuppone comunque l'individuazione del fine

[20] Cfr L. D'Andrea E. Morriconi, *Controlli a Distanza: La Disciplina Prima e Dopo la Riforma,* Op cit. pp. 10-13.

per cui essa è realizzata, oltre che, ovviamente dell'operatività e del funzionamento concreti dello strumento. Quindi nel momento in cui l'impiego è lecito il datore di lavoro può adoperarsi nello strumento anche in maniera occulta per andare ad accertarsi del fatto illecito.

Questa interpretazione letta in combinato disposto con l'approccio giurisprudenziale relativo ai controlli difensivi ante riforma, ci permette di chiarire in quali casi siano o meno legittimi i controlli preterintenzionali (ovvero quelli che tendono a soddisfare esigenze non inserite inizialmente nell'accordo sindacale, che si presentano in corso d'opera). I controlli difensivi e il relativo filone giurisprudenziale si presume possa rimanere operativo per quanto riguarda il momento dell'impiego ovvero il sussistere di una finalità concreta.

In definitiva non possiamo non ribadire nuovamente che la ratio della norma è quella di andare ad allentare la pressione nei confronti del datore di lavoro e non il contrario.

Sull'interpretazione in questione Alvino non si pone il dubbio sul problema derivante tra impiego e installazione, ma ritiene che di fatto vadano di pari passo e di conseguenza nel momento in cui l'impiego è lecito è lecita anche l'installazione.[21]

Secondo Del Punta, l'inserimento di "tutela del patrimonio aziendale" ha come scopo quello di superare il concetto di controllo difensivo, in particolare nella versione estrema che veniva esentato dalla procedura autorizzativa. Infatti egli ritiene che l'illecito si configuri se lo strumento venisse installato senza l'autorizzazione o l'accordo. Di conseguenza secondo Del Punta questo porterebbe di fatto alla fine dei c.d. "controlli difensivi" quando posti in essere senza accordo o autorizzazione. Un'altra semplificazione riguarda la possibilità

[21] Cfr, I. Alvino, Labour & Law Issues, *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*, Op Cit. p.15.

per le imprese con unità produttive dislocate in più province ovvero in più regioni l'accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In pratica l'impresa può scegliere di confrontarsi una volta sola a livello nazionale con le associazioni sindacali più rappresentative concludendo un accordo che vale per tutte le unità dislocate sul territorio.

Un'analoga semplificazione è prevista in riferimento alla procedura autorizzativa in sede amministrativa, cui l'impresa può ricorrere in mancanza di accordo: invece che passare da ciascuna DTL può rivolgersi direttamente al Ministero del Lavoro e delle politiche sociali. In merito a queste semplificazioni si ritiene che non comporta che l'impresa debba percorrerle entrambe prima di poter ritenere realizzata quella "mancanza di accordo" che la abilita a richiedere l'autorizzazione amministrativa. [22]

[22] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, Op cit., p.11

2.2 Gli strumenti di lavoro

Il secondo comma dell'art. 4 non trovava esplicita regolazione nel vecchio testo normativo che, come visto, andava semplicemente a dettare le condizioni per l'installazione delle apparecchiature di controllo. Il secondo comma esclude totalmente dalla procedura di cui il primo comma gli strumenti di lavoro per rendere la prestazione lavorativa e gli strumenti per la registrazione degli accessi e delle presenze.

Il secondo comma della norma, rappresenta la risposta del legislatore all'obsolescenza informatica del vecchio testo, che, come abbiamo visto, costringeva a domandarsi con risposte differenziate da parte della prassi e della giurisprudenza (con anche il rischio di un provvedimento penale) se per assegnare a un lavoratore un normalissimo computer o per installare un badge fosse necessario procurarsi un accordo sindacale.

Una prima domanda che subito ci poniamo è cosa si intenda per strumenti di lavoro per rendere la prestazione lavorativa ovvero il Legislatore vuole includere solo ciò che di fatto viene utilizzato per rendere la prestazione oppure anche tutto ciò che viene fornito dall'azienda per rendere possibile la prestazione? Pensiamo ad esempio ad uno smartphone dato in uso al lavoratore.

Per fornire una risposta a tale domanda si deve ragionare sulle due caratteristiche che uno strumento di lavoro deve possedere:

- lo strumento deve essere utilizzato dal lavoratore;
- lo strumento deve essere utilizzato per rendere la prestazione lavorativa;

Il primo requisito include solo gli strumenti utilizzati del lavoratore, ossia quegli strumenti che necessitino di una partecipazione attiva del lavoratore.

Il secondo requisito prevede che lo strumento sia un mezzo utile e funzionale allo svolgimento della mansione oggetto del contratto con il lavoratore. In questa prospettiva è facile includere quindi i computer e gli smartphone ma non

eventuali applicativi o strumenti che consentano di monitorare momento per momento l'attività del lavoratore.

E allora la seconda domanda che ci poniamo è la seguente: se all'interno del dispositivo fossero già presenti degli strumenti che consentono di rilevare e quindi controllare l'attività del lavoratore? Basti pensare al GPS oramai presente nella maggior parte dei dispositivi.

Facciamo un esempio: immaginiamo che un datore di lavoro che fornisce un servizio di assistenza a chiamata ai suoi clienti voglia utilizzare autovetture dotate di GPS per poter determinare nel minor tempo possibile quale sia l'autovettura più vicina alla zona di richiesta. In questo caso il GPS si può ritenere uno strumento di lavoro e quindi rientrare nel novero del secondo comma? In questo caso si, perché il GPS è essenziale per trarre il massimo vantaggio dalla prestazione lavorativa. Discorso diverso sarebbe se il GPS venisse utilizzato per prevenire furti all'autovettura, e quindi in questo caso rientrerebbe nell'applicazione del 1° comma.

A conferma di quanto appena esposto si riporta l'interpretazione fornita dal Ministero del Lavoro e delle politiche sociali, che con nota del 18 giugno 2015 chiarisce la norma nel seguente modo: "«l'espressione «*per rendere la prestazione lavorativa*» comporta che l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale mezzo che "serve" al lavoratore per adempiere la prestazione: ciò significa che, nel momento in cui tale strumento viene modificato (ad esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione: in tal caso, infatti, da strumento che "serve" al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore per controllarne la prestazione. Con la conseguenza che queste "modifiche" possono *avvenire solo alle condizioni*

ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione.[23]

Alla luce di questa interpretazione quindi il lavoratore a cui è stato dato uno smartphone con la localizzazione GPS può essere controllato se si è recato dal cliente solo se quest'informazione è ricavabile senza installare altri applicativi ad hoc. In caso contrario, l'installazione di ulteriori parti hardware o software che consentissero il controllo del lavoratore ricadrebbero nel novero di quanto affermato dal Ministero del Lavoro e quindi installabili solo a seguito dell'accordo sindacale. Quindi potremmo avere interpretazioni diverse da parte della giurisprudenza che potranno andare a consentire controlli tramite dispositivi che per come sono stati prodotti ne consentono il controllo. Del Punta in merito ritiene che, per rimanere fuori dal primo comma della norma, ci debba essere una stretta correlazione tra gli strumenti tecnologici e le mansioni svolte dal lavoratore. Posto che per strumenti è evidente che vi rientrino anche i *software* secondo questa impostazione di Del Punta nell'esempio precedente non si potrebbe utilizzare il GPS, anche se già presente nel dispositivo, se di fatto non è utile al fine di rendere la prestazione. Quindi in caso di utilizzo necessiterebbe dell'accordo o dell'autorizzazione. Questo anche perché altrimenti potrebbe potenzialmente rientrare tutto nel novero del secondo comma, lasciando al primo comma spazio per le sole telecamere. È chiaro che è arduo riuscire a tracciare un confine preciso tra ciò che serve per lavorare e ciò che serve a rendere più efficiente e/o sicura la singola prestazione (2° comma), e ciò che serve a rendere più efficiente e/o sicura l'organizzazione del lavoro, con benefici sulla prestazione lavorativa (1° comma). .[24]

È bene precisare che l'installazione dello strumento è ben distinta dalla possibilità di utilizzare le informazioni dallo stesso registrate. Infatti il datore di

[23] L.D'andrea E. Morriconi, *Controlli a Distanza: La Disciplina Prima e Dopo la Riforma*, Op Cit. p. 14.
[24] R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, Op cit., p.14-15

lavoro non deve ritenersi libero di esaminare i dati in quanto dovrà andare a rispettare quanto stabilito dal terzo comma del nuovo articolo, anche questo di nuova introduzione, che prevede il rispetto della normativa riguardante la privacy.

Per concludere sul tema degli strumenti di lavoro è interessante soffermarsi su una apparecchiatura tecnologica di recente diffusione il BYOD (*bring your own device*).[25]

Questo strumento consente di creare sul dispositivo di proprietà del dipendente due ambienti diversi, contenenti dati aziendali e dati personali. In questa ipotesi dunque lo strumento è di proprietà del lavoratore, ma viene utilizzato avvalendosi di un applicativo di proprietà del datore di lavoro.

Questo strumento sta avendo una grande diffusione e quindi necessita una riflessione se possa essere incluso negli strumenti di lavoro oppure no.

Infatti, all'interno del dispositivo, ci saranno sicuramente molte informazioni personali in quanto l'utente ne fa l'uso sia personale sia lavorativo, se ne fosse consentito il controllo si potrebbe avere molte più informazioni meritevoli di tutela rispetto al caso in cui lo strumento fosse di proprietà del datore di lavoro.

L'articolo non introduce distinzioni in merito alla proprietà del dispositivo, inserisce nella categoria degli strumenti di lavoro tutti quelli utilizzati dal lavoratore per rendere la prestazione. Dunque se ne evince che lo strumento possa essere installato purché vi sia il consenso del lavoratore e purché sia funzionale allo svolgimento della prestazione lavorativa. Quindi si ritiene che sia

[25] Cfr, [25] I. Alvino, Labour & Law Issues, *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*, Op cit. pp.22-26.

possibile purché vi siano gli accorgimenti utili ad evitare che le informazioni personali siano visibili dal datore di lavoro[26].

A modesto parere di chi scrive si ritiene tuttavia che l'installazione dell'applicativo BYOD possa rientrare nel novero del primo comma dell'art. 4 in quanto non presente di default nel dispositivo questo anche alla luce dell'interpretazione fornita dal Ministero del lavoro come precedentemente riportato.

[26] Cfr, I. Alvino, Labour & Law Issues, *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*, Op Cit. pp. 22-26.

2.3 Gli strumenti di registrazione degli accessi e delle presenze.

Oltre alla non applicabilità del primo comma dell'art. 4 per gli strumenti di lavoro, questo non è applicabile anche per quanto riguarda la registrazione degli accessi e delle presenze. Questa scelta è ritenuta pienamente condivisibile in quanto l'informazione sull'orario di ingresso e di uscita non è un monitoraggio della prestazione lavorativa, ma soltanto informazione sull'inizio e la fine della prestazione senza andare a ledere la dignità del lavoratore. In questa sede un dubbio si pone in riferimento agli strumenti di rilevazione degli accessi a specifici locali aziendali ovvero degli strumenti utili a registrare il passaggio da un locale a un altro, dove la finalità è quella di individuare il personale presente in una determinata area in un certo momento. Gli strumenti a cui si fa riferimento sono ad esempio il Badge aziendale, ovvero una tessera magnetica che consente di registrare l'ingresso del lavoratore. Vi rientrano i *dati biometrici* ovvero quei dati ricavabili tramite il "corpo" come la lettura della retina, l'impronta digitale. Inoltre vi rientra la tecnologia *"Rfid"* ovvero un dispositivo che consente di identificare, anche senza l'uso di telecamere, se un lavoratore è presente in una determinata area o no. In merito a questi strumenti troveremo i dettagli nel capitolo 4 di questa tesi.

In questa sede ci si chiede se l'installazione di questi apparecchi necessiti l'autorizzazione ai sensi del primo comma. Tuttavia per come la norma è stata scritta la congiunzione "e" non lascia spazio molteplici interpretazioni consentendo di fatto di adoperarsi di qualsiasi strumento utile alla rilevazione della presenza e dunque di controllo del rispetto dell'orario di lavoro.[27]

[27] Cfr, I. Alvino, Labour & Law Issues, *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*, Op cit. pp. 20-23.

2.3 L’informativa da fornire ai lavoratori.

Come abbiamo precedentemente analizzato nel capitolo 1 si evidenziava la problematica relativa all’utilizzo delle informazioni ricavate da parte del datore di lavoro nei confronti dei lavoratori a seguito dei controlli. Infatti il progresso tecnologico ha portato a fattispecie in cui è possibile avere informazioni personali del lavoratore. Il problema era dovuto anche dal fatto che l’art. 4 non richiamava in alcun modo la disciplina sulla privacy. Quest’assenza di regole relativa alle modalità di utilizzo dell’informazione raccolte aveva portato da una parte il caso in cui l’accordo sindacale inibisse la successiva utilizzazione delle informazioni raccolte determinando così il controverso comportamento da parte dei datori di lavoro che preferivano non stipulare accordi ed eventualmente appoggiarsi, in caso di necessità, al filone giurisprudenziale dei controlli difensivi.

Questo problema è stato risolto inserendo come norma positiva il comma 3 che recita: “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”***.

Questo ci permette di fare le seguenti considerazioni, ovvero il datore di lavoro non ha bisogno di alcuna autorizzazione per poter controllare gli strumenti di lavoro, tuttavia questo non è consentito se non viene data preventivamente apposita informativa al lavoratore secondo quanto stabilito dall’art. 13 della normativa sulla privacy. Inoltre si consente l’utilizzazione dei dati registrati a tutti i fini connessi al rapporto di lavoro, da uno degli strumenti appartenenti alle categorie enucleate ai commi primo e secondo. Si riporta l’art.13 del codice della privacy relativamente all’informativa da fornire ai lavoratori:

Art. 13 (Informativa) - Codice privacy

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'articolo 7;

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di

Art. 13 (Informativa) - Codice privacy

assistenza e informazione al pubblico.

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando: *a)* i dati sono trattati in base ad un obbligo previsto dalla L., da un regolamento o dalla normativa comunitaria; *b)* i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla L. 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; *c)* l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

5-*bis*. L'informativa di cui al comma 1 non è dovuta in caso di ricezione di *curricula* spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere *a*), *d*) ed *f*).

Il datore di lavoro si dovrà attenere alla soprariportata informativa nel caso in cui voglia monitorare gli strumenti di lavoro e prima di installare eventuali

telecamere. Per quanto riguarda l'utilizzo delle informazioni il datore di lavoro sarà soggetto a tre ordini di limitazioni:

- Quelli previsti dall'accordo stipulato con il sindacato o dall'autorizzazione della DTL
- Che il datore di lavoro abbia fornito l'informativa adeguata al lavoratore
- Che i controlli avvengano nel rispetto della L. sulla privacy.

Ne deriva che anche il controllo fatto secondo il principio dei controlli difensivi dovrà essere sottoposto a preventiva informativa dei lavoratori, altrimenti non sarà valido il controllo effettuato. Questo porta senza dubbio un giusto bilanciamento nei rapporti fra il datore di lavoro e il lavoratore, in quanto si ha una certezza normativa che pone l'obbligo di informazione ai lavoratori che non può essere derogato se non forse nella contrattazione di prossimità. L'informativa diviene condizione necessaria per l'utilizzo dei dati recepiti dal lavoratore.

È chiaro che il concetto di "adeguatezza" farà gravitare intorno a sé il contenzioso giudiziario futuro, in quanto non si comprende bene cosa si intenda nel concreto. È evidente che l'informativa dovrà essere completa e dettagliata, ricomprendo tutti gli strumenti, tanto di lavoro quanto di mero controllo.[28]

Relativamente alle modalità di utilizzo dei dati divengono fondamentali le prescrizioni rilasciate dal Garante della Privacy che ha il compito di fornire le modalità e i limiti secondo cui queste informazioni possono essere usate. Se le modalità stabilite dal Garante non venissero rispettate questo verrebbe considerato come una violazione del Codice.[29]

[28] A. Bottini, "Necessari regolamenti aziendali dettagliati, chiari e completi", *Il sole 24 ore*, 24 agosto 2016, p.28

[29] Cfr, I. Alvino, Labour & Law Issues, *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*, Op Cit. pp. 28-31.

Il Codice della Privacy ha stabilito i principi secondo cui questi dati possono essere utilizzati:

- Necessità
- Correttezza
- Trasparenza
- Pertinenza
- Non eccedenza

Il principio di necessità obbliga il datore di lavoro ad utilizzare quegli strumenti di controllo che siano strettamente necessari e porre in campo le misure idonee a ridurre al minimo la necessità di effettuare i controlli utilizzando degli applicativi o software che limitino ad esempio la liberta di utilizzo di internet impedendo l'accesso a determinati siti.

La correttezza e la trasparenza esplica l'onere di rendere noti ai lavoratori i controlli che potranno essere eventualmente fatti utilizzando, come detto in precedenza, l'informativa sulla privacy. [30] Inoltre dovrà essere data anche informazione relativa, ad esempio, alla possibilità di scaricare musica sul computer di avere una cartella personale e quant'altro.

Il principio di non eccedenza è da L.re insieme al principio di necessità ci sono i rimanenti principi di pertinenza e di non eccedenza, in cui il Garante vieta la possibilità di eseguire controlli prolungati, costanti e indiscriminati ed evidenzia la necessità di intervenire con accorgimenti tecnici lasciando quindi solo come ultima possibilità quella dei controlli individuali. Infine l'autorità garante pone l'obbligo alle aziende di istituire programmi che prevedano la cancellazione dei dati relativi all'accesso a internet e al traffico telematico.

[30] L.D'andrea E. Morriconi, *Controlli a Distanza: La Disciplina Prima e Dopo la Riforma*, Op Cit. p. 18.

Relativamente alla locuzione del comma "informazione adeguata" bisogna capire cosa si intenda per adeguata e sicuramente possono risultare d'aiuto le linee guida fornite dal Garante che afferma: "*grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli […] Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative*".

Quindi si dovrà valutare caso per caso se l'informazione fornita al lavoratore sia stata adeguata considerando l'idoneità della stessa di mettere a conoscenza il lavoratore, in maniera dettagliata, dovrà indicare almeno:

- Quali sono gli strumenti, presenti in azienda, o utilizzati direttamente o indirettamente dal lavoratore, dai quali può derivare una possibilità di controllo,
- Quali sono le modalità con le quali è possibile utilizzare gli strumenti forniti dal datore di lavoro,
- Le modalità secondo cui potranno essere eseguiti dei controlli sui dati registrati dallo strumento installato in azienda o utilizzato dal lavoratore.

Non appare invece necessario ricordare a eventuali risvolti disciplinari nel caso di condotte vietate.[31]

È importante sottolineare che il datore di lavoro deve dare prova che il lavoratore è stato messo a conoscenza e che è stata recepita dal lavoratore utilizzando mezzi

[31] I. Alvino, Labour & Law Issues, *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*, Op Cit. p.34.

che provino l'avvenuta ricezione dell'informativa. Questo non è da confondere con il consenso per l'utilizzo dei dati personali di cui è lecito porsi il dubbio. Infatti riteniamo che quest'informativa e il trattamento dei dati non rientri nel campo di applicazione dell'art.23 d.lgs. 196/2003 ma uno dei casi in cui il Codice della privacy ne esclude la necessità di acquisire il consenso. Questo viceversa non è valido nel caso in cui il datore di lavoro avesse la possibilità di accedere a informazioni come opinioni politiche orientamento sessuale e religioso, in questo caso non è possibile utilizzare l'informazione per qualsiasi fine anche se il lavoratore avesse rilasciato il consenso. L'unico caso in cui potrebbe essere utilizzato è nel caso in cui il diritto da tutelare sia di rango pari a quello dell'interessato e quindi rientrante nell'art. 26 comma 4 lett. c del d.lgs. 196/2003.[32]

L'informativa, chiamata anche policy aziendale, dovrà essere aggiornata ogni qual volta dovessero essere modificati gli strumenti di lavoro rispettando le disposizioni viste sopra.[33]

In riguardo alle informazioni raccolte, il nuovo art. 4 stabilisce che sono utilizzabili a tutti i fini connessi al rapporto di lavoro. Questo prevede che per poter irrogare sanzioni disciplinari è necessario innanzitutto aver dato l'informativa in maniera adeguata ai lavoratori. In secondo luogo è opportuno ricordare che è necessario rispettare anche l'art. 7 dello statuto dei lavoratori. Ovvero prevedere un codice disciplinare e all'interno del documento prevedere che:

- le infrazioni a cui possono essere applicate sanzioni;
- le sanzioni che si applicano a ciascuna infrazione;

[32] I. Alvino, Labour & Law Issues, *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*, Op Cit. pp.35-36.
[33] A. Bottini, "Dipendenti informati su telecamere e tablet", *Il sole 24 ore*, 24 agosto 2016, p.28

- applica quanto previsto in merito anche dai contratti collettivi
- deve essere affisso in un luogo accessibile a tutti i lavoratori.

Questo non è da confondere con la policy aziendale che fornisce come abbiamo visto informazioni in merito all’utilizzo dei dati ottenuti attraverso gli strumenti di controllo.

2.4 Il regime transitorio.

In questo paragrafo tratteremo il regime transitorio ovvero i casi in cui vi fosse un accordo sindacale tra le parti stipulato secondo le vecchie regole del Jobs Act.

In particolare una prima domanda che ci poniamo è in merito all'informativa da dare ai lavoratori. Infatti, come abbiamo visto nel precedente paragrafo, il datore di lavoro deve dare adeguata informazione ai lavoratori dei controlli che potrebbero essere effettuati. Quindi su questo punto nel caso in cui ci fosse stato un accordo con il sindacato ma non fosse stata data adeguata informativa si possono ritenere comunque validi gli eventuali controlli effettuati?

Si ritiene che il datore di lavoro dovrà comunque fornire l'informativa ai lavoratori anche per gli accordi stipulati in precedenza per due ragioni: da un lato, il nuovo art. 4 non introduce alcuna disposizione rispetto ai controlli installati prima o dopo l'entrata in vigore della norma. Dall'altro l'adempimento informativo può essere svolto autonomamente dal datore di lavoro senza che vi sia alcuna cooperazione da parte di altri soggetti. Per queste ragioni riteniamo che le aziende dovranno adeguarsi nel caso in cui dovessero utilizzare gli strumenti di controllo installati prima della riforma.[34]

Inoltre un'altra domanda da porsi è relativa agli accordi collettivi sottoscritti a livello aziendale sotto il vigore del vecchio art. 4 quindi chiedersi se la nuova disciplina vada a intaccare anche sugli accordi precedenti oppure se questi possono essere ritenuti ancora validi. Su questo punto non è possibile dare una risposta precisa però su può affermare che la nuova disposizione non ha un effetto immediato di caducazione del vecchio accordo se questo è compatibile con il nuovo articolo.

[34] I. Alvino, Labour & Law Issues, *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*, Op Cit. p.37.

Sicuramente, visto la nuova impostazione della norma relativa agli strumenti di lavoro, i datori di lavoro potrebbero avere interesse a sciogliere l'accordo per potere rientrare nelle nuove regole del Jobs Act.[35]

2.5 I problemi relativi alla contrattazione di prossimità.

"I contratti di prossimità sono disciplinati dall'art. 8 del D.L. n. 138/2011 (convertito in L. dalla l. n. 148/2011 ed in vigore dal 17 settembre 2011), volto a regolamentare la materia della contrattazione aziendale/territoriale. Si tratta di contrattazione di secondo livello, aziendale o territoriale, ed ha in genere la funzione di integrare il CCNL per meglio rispondere ai bisogni della singola azienda o delle aziende di una determinata aerea territoriale. Bisogna premettere che il contratto di prossimità si caratterizza per il fatto che la funzione normativa, abilitata a derogare a disposizioni inderogabili, svolge un ruolo strumentale rispetto all'obiettivo prestabilito che l'accordo è diretto a perseguire."[36]

Come spiega in maniera esauriente la pagina di Wikipedia i contratti di prossimità servono ad integrare il CCNL con lo scopo di andare a risolvere specifiche problematiche specifiche per una determinata azienda. Al secondo comma dell'art.8 vengono inserite le specifiche materie su cui si può derogare al CCNL e all'art 4 dello Statuto dei Lavoratori di cui si riporta il testo: *"2. Le specifiche intese di cui al comma 1 possono riguardare la regolazione delle materie inerenti l'organizzazione del lavoro e della produzione con riferimento:*

a) agli impianti audiovisivi e alla introduzione di nuove tecnologie;

b) alle mansioni del lavoratore, alla classificazione e inquadramento del personale;

---

[35] I. Alvino, Labour & Law Issues, *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*, Op cit. p.38.

[36] *Contratto di prossimità* - https://it.wikipedia.org

c) ai contratti a termine, ai contratti a orario ridotto, modulato o flessibile, al regime della solidarietà negli appalti e ai casi di ricorso alla somministrazione di lavoro;

d) alla disciplina dell'orario di lavoro;

e) alle modalità di assunzione e disciplina del rapporto di lavoro, comprese le collaborazioni coordinate e continuative a progetto e le partite IVA, alla trasformazione e conversione dei contratti di lavoro e alle conseguenze del recesso dal rapporto di lavoro, fatta eccezione per il licenziamento discriminatorio, il licenziamento della lavoratrice in concomitanza del matrimonio, il licenziamento della lavoratrice dall'inizio del periodo di gravidanza fino al termine dei periodi di interdizione al lavoro, nonché fino ad un anno di età del bambino, il licenziamento causato dalla domanda o dalla fruizione del congedo parentale e per la malattia del bambino da parte della lavoratrice o del lavoratore ed il licenziamento in caso di adozione o affidamento.

2-bis. Fermo restando il rispetto della Costituzione, nonché i vincoli derivanti dalle normative comunitarie e dalle convenzioni internazionali sul lavoro, le specifiche intese di cui al comma 1 operano anche in deroga alle disposizioni di L. che disciplinano le materie richiamate dal comma 2 ed alle relative regolamentazioni contenute nei contratti collettivi nazionali di lavoro."[37]

Il Legislatore del 2011 di fronte alla difficoltà di elaborare una disciplina normativa in materia di controlli a distanza, aveva ritenuto di rimettere alle parti sociali il potere di andare a derogare l'art. 4 dello statuto dei lavoratori.

[37] *Contratto di prossimità - https://it.wikipedia.org*

Andremo adesso ad analizzare i problemi che possono nascere fra il nuovo art. 4 dello statuto dei lavoratori e l'art.8 della predetta L.. In particolare analizzeremo il problema sotto 2 profili: 1) i soggetti della contrattazione di prossimità in rapporto alle rappresentanze sindacali, 2) ai profili relativi ai controlli a distanza sui quali la contrattazione di prossimità può intervenire e i limiti che questa incontra rispetto alle regole derogatorie.

Relativamente al primo profilo, l'art.8 amplifica la platea dei soggetti abilitati a stipulare un accordo con il datore di lavoro per consentire un controllo a distanza dell'attività dei lavoratori. Infatti l'art. 4 prevede l'ampliamento della platea solo nel caso in cui l'azienda si trovi nella situazione di essere un'azienda plurilocalizzata. Per come posto l'art.8 prevede un allargamento anche per le piccole aziende che non hanno necessariamente rappresentanze sindacali all'interno. Il problema è relativo all'area in cui si può intervenire in tal senso. Ad esempio si potrebbe prevedere secondo questa interpretazione un accordo territoriale che regolamenti il controllo a distanza dei lavoratori per le imprese artigiane aderenti associazioni datoriali stipulanti l'accordo. Per quanto riguarda i limiti, il citato art 8 pone due categorie di limiti alle quali deve attenersi l'autonomia collettiva: 1) l'intesa deve essere finalizzata a perseguire uno degli obbiettivi individuati nella disposizione 2) l'intesa non può andare in contrasto con la costituzione e con i vincoli delle normative comunitarie e delle convenzioni internazionali sul lavoro.[38]

A questo punto ci chiediamo quali sono le regole del nuovo art. 4 dello Statuto dei Lavoratori che possono oggi essere derogate dal contratto di prossimità? Innanzitutto si potrebbe ipotizzare che tramite il contratto di prossimità si vada ad ampliare gli strumenti per i quali non è necessario l'ottenimento della preventiva autorizzazione per l'installazione di ulteriori applicativi o software nei

[38]Cfr, I. Alvino, Labour & Law Issues, *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*, pp.38-41.

dispositivi dati in uso ai lavoratori. Allo stesso modo il contratto di prossimità potrebbe ridurre l'innovazione stabilita dall'art. 4 dello statuto dei lavoratori imponendo l'acquisizione preventiva dell'autorizzazione anche nei casi in cui non sia necessaria. Si tratta quindi di libera contrattazione fra le parti.

Per quanto riguarda il secondo profilo le domande da porsi sono:

- il contratto di prossimità può autorizzare l'installazione di strumenti per finalità di controllo a distanza dell'attività dei lavoratori?
- Il contratto di prossimità può sollevare il datore di lavoro dall'onere di fornire adeguata informativa ai lavoratori sulle modalità di controllo?
- Il contratto di prossimità può escludere o ridimensionare l'applicazione derivanti dai principi del codice della privacy?

Le risposte non sono semplici o comunque potrebbero esserci casi diversi e quindi non una risposta univoca. In ogni caso si può individuare 2 punti fermi. Il primo è che non sarà mai possibile l'installazione di strumenti il cui fine sia quello del controllo dell'attività lavorativa. Questa conclusione è dovuta al fatto che la possibilità di istituire un controllo a distanza continuativo è consentito solo nel caso in cui questo sia necessario per interessi maggiori di tutela. Quindi il fine esclusivo del controllo del lavoratore deve essere accompagnato da una motivazione che vada nell'interesse di quest'ultimo. Inoltre si può fare anche un'altra osservazione, ovvero essendo l'art. 4 assistito da norme penali, non sarebbe possibile rimuovere una fattispecie di reato autorizzando comportamenti altrimenti illeciti.

Il secondo punto fermo riguarda il rapporto tra l'impiego dei mezzi tecnologici e la protezione della riservatezza del lavoratore e in particolare alla forza che deve essere attribuita ai principi dettati dal Codice della Privacy. Sotto questo profilo si può affermare che il contratto di prossimità non potrebbe autorizzare il datore

di lavoro ad operare controlli sul lavoratore senza rispettare i limiti posti dal Codice della privacy, come più sopra ricostruiti.

Si arriva a questa conclusione anche perché non si può pensare che il potere di deroga possa arrivare al punto di surclassare una norma pensata per tutelare diritti di rango costituzionale. Quindi in ogni caso non si potrà andare contro i principi di necessità, correttezza, trasparenza e non eccedenza. Invece si ritiene che per quanto riguarda l'informativa possa essere variata purché siano messi a disposizione del lavoratore strumenti idonei a garantire la conoscenza della possibilità di controllo in ottemperanza del principio di trasparenza.[39]

[39] Cfr I. Alvino, Labour & Law Issues, *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*, Op. Cit. pp.41-43.

2.6 Le Sanzioni dello Statuto dei Lavoratori

Il nuovo art. 4 al comma 3, come già visto, fa esplicito richiamo alla normativa della privacy. Il Codice della Privacy dedica un apposito articolo ai controlli a distanza con l'art.114 il quale si limita ad affermare che " resta fermo quanto disposto dall'art. 4 della L. 300/70". Sempre lo stesso codice, con l'art.179, ha soppresso nell'art.38 della L. 300/70 (relativo alle disposizioni penali) il riferimento all'art. 4, per cui già prima della modifica apportata dal D.Lgs. n. 151/2015, la sanzione per il mancato rispetto dell'art.114 del codice della privacy, e quindi anche dell'art. 4 della L. 300/70, era quella stabilita dall'art. 171 del Codice il quale prevedeva che la violazione della disposizione di cui all'art.114 era punita con la sanzione di all'art.38 della L. 300/70.

Di fatto quindi non è cambiato nulla in quanto la sanzione da applicare in caso di mancato rispetto dell'art. 4 resta sempre quella prevista dall'art.38 che punisce con l'ammenda da 154€ fino a 1549€ o con l'arresto da 15 giorni ad un anno l'installazione di sistemi di videosorveglianza:

- Finalizzati al mero controllo a distanza dei lavoratori;
- Aventi finalità diverse dal mero controllo dei lavoratori ma senza il previo accordo delle RSU/RSA o l'autorizzazione della DTL .

Nei casi più gravi la pena dell'arresto e dell'ammenda sono applicati congiuntamente.

La Direzione Generale dell'Attività Ispettiva del Ministero del lavoro, con nota n. 4343 del 4 ottobre 2006, rispondendo ad un quesito formulato sull'applicabilità della prescrizione obbligatoria in presenza di violazioni penalmente sanzionate ai sensi dell'art.38, L. 300/70, ha chiarito che spetta all'ispettore, quale primo osservatore della fattispecie concreta, il potere dovere di individuare i casi di maggiore gravità e quindi di applicare o meno l'istituto della prescrizione.

In merito a questo il Ministero, ha precisato che l'art. 4 dello Statuto dei Lavoratori, al comma 1 (vecchio testo), con l'inciso "apparecchiature per finalità di controllo a distanza dei lavoratori" richiama il dolo intenzionale del contravventore che installi sistemi di video sorveglianza al solo fine del controllo a distanza dell'attività dei lavoratori, mentre il comma 2 (vecchio testo e comma 1 dell'attuale testo) fa riferimento ad un atteggiamento quantomeno colposo dello stesso datore.

La Direzione Generale ha cercato di esemplificare le possibili violazioni dell'art. 4 che sono caratterizzate da maggiore gravità e che non consentono, l'applicazione dell'istituto della "prescrizione obbligatoria" che di seguito elenchiamo:

- Installazione di telecamere fisse che inquadrino esclusivamente l'attività svolta dai lavoratoriovvero i luoghi adibiti esclusivamente al godimento della pausa, nonché alla consumazionedel pasto da parte degli stessi;
- Assenza di esigenze organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale che rendano necessaria l'installazione degli strumenti di controllo a distanza;
- Installazione degli impianti a totale insaputa del lavoratore. Non v'è dubbio, difatti, che tale installazione sia maggiormente insidiosa, e la condotta del datore sia maggiormente idonea a mettere in pericolo la riservatezza del lavoratore così come più volte affermato anche dalla Suprema Corte.
- Devono considerarsi, inoltre, particolarmente insidiosi quei sistemi di controllo che, considerata la relativa collocazione ovvero la specifica funzionalità, siano in grado di raccogliere in via prevalente i dati c.d. "sensibili" del lavoratore così come individuati dal Codice della Privacy (D.Lgs. n. 196/2003) quali, ad esempio, i dati idonei a rilevare le origini razziali, le condizioni sanitarie o lo stato di salute, l'appartenenza politica

o sindacale, la vita o le abitudini sessuali, la sfera psichica, il credo religioso, definire il profilo o la personalità del lavoratore, ecc. .

- Vanno, inoltre, annoverate nelle ipotesi di maggiore gravità tutte quelle circostanze che non solo hanno messo in pericolo la libertà individuale del lavoratore, ma che hanno altresì comportato un effettivo danno allo stesso, quali, ad esempio, le registrazioni e/o l'utilizzazione (a qualunque fine) delle immagini riprese dai sistemi audiovisivi installati dal trasgressore (sarebbe, infatti, indice di un maggior disvalore della condotta del datore di lavoro l'utilizzazione delle immagine che abbiano facilitato atteggiamenti mobbizzanti nei confronti dei lavoratori, ovvero, che abbiano determinato l'adozione di provvedimenti disciplinari).

Si ritiene che le indicazioni in questione siano assolutamente valide anche alla luce del nuovo art. 4 per cui i casi di maggiore gravità siano quelli in cui i sistemi di videosorveglianza, siano installati per mere finalità di controllo a distanza dei lavoratori.[40]

[40] Cfr, R. Schiavone, Controllo *dei Lavoratori*, Op Cit, pp. 36-38

3. IL CODICE DELLA PRIVACY

In questo capitolo forniremo un'infarinatura generale sul codice della privacy e sulle Linee Guida fornite in materia al trattamento dei dati, vedremo le fonti alla base dei diritti della privacy. Analizzeremo gli aspetti concreti dovuti all'informativa da fornire, il responsabile del trattamento, l'incaricato e l'amministratore di sistema. Questo capitolo è molto importante alla luce dell'espresso richiamo che viene fatto dall'art. 4 dello S.L al Codice della Privacy e anche perché, nel capitolo successivo, tratteremo in dettaglio le problematiche che si potranno avere in relazione ai controlli che il datore di lavoro vorrà mettere in atto.

3.1 Le fonti alla base dei diritti della privacy dei lavoratori

Il diritto alla privacy nell'ambito del rapporto di lavoro è un diritto di rango costituzionale tutelato dagli art.2 e 3 e in particolare, per quanto riguarda la sfera lavorativa, dall'art. 41 il quale riconosce la libertà di iniziativa economica e privata ma pone al datore di lavoro imprenditore il rispetto della sicurezza, della libertà, e della dignità umana del prestatore di lavoro.

In realtà in ordine di tempo ancora prima della Costituzione era il Codice Civile all'art.2087, che già si occupava di tutelare le condizioni del lavoratore obbligando l'imprenditore a porre in atto le misure necessarie a tutelare l'integrità fisica e la personalità morale dei lavoratori.[41] Ad una vera e propria legislazione sul diritto di riservatezza ci si è arrivati proprio con la L. 300 del 20 maggio 1970 che si prefiggeva lo scopo di andare a creare un clima di rispetto della dignità e libertà umana nei luoghi di lavoro. Essenziale è l'art.8 che vieta al datore di lavoro di poter compiere indagini anche a mezzo di terzi su opinioni politiche religiose o sindacali del lavoratore.

[41] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.116

Il codice della privacy venne emanato con D.lgs. n. 196 del 30 giugno 2003 per disciplinare in modo esaustivo il trattamento dei dati personali compresi quelli nel rapporto di lavoro.

Inoltre è importante ricordare il quadro Europeo con:

- La carta dei diritti fondamentali dell'Unione Europea che all'art.8 riconosce ad ogni individuo il diritto alla protezione dei dati di carattere personale.
- La direttiva 95/46/-ce del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- La direttiva 2002/58/Ce relativa al trattamento dei dati personali e alla tutela della privata nel settore delle comunicazioni elettroniche.
- Il recentissimo Regolamento emanato dalla comunità Europea il 27/04/2016 n. 2016/679

Il 23 novembre 2006 il Garante per la protezione dei dati personali ha fornito delle linee guida in merito al trattamento dei dati personali. Con queste Linee Guida si è così preceduto alla definizione di un quadro unitario di misure e di accorgimenti necessari ed opportuni al fine di fornire orientamenti utili per i datori di lavoro relativamente al trattamento dei dati personali connessi al rapporto di lavoro individuando i comportamenti più appropriati da adottare.[42]

[42] Cfr R. Schiavone, Controllo *dei Lavoratori*, Op Cit., pp.117-119.

3.2 I dati riguardanti i lavoratori

Nello svolgimento del rapporto di lavoro il datore di lavoro tratta soprattutto i seguenti dati:

- dati anagra• ci di lavoratori (assunti o cessati dal servizio), dati biometrici, fotogra• e e dati sensibili riferiti anche a terzi, idonei in particolare a rivelare il credo religioso o l'adesione a sindacati;
- dati idonei a rivelare lo stato di salute, di regola contenuti in certi• cati medici o in altra documentazione prodotta per giusti• care le assenze dal lavoro o per fruire di particolari permessi e bene• ci previsti anche nei contratti collettivi;

informazioni più strettamente connesse allo svolgimento dell'attività lavorativa, quali:

- la tipologia del contratto
- la qualifica e il livello professionale
- la retribuzione individuale corrisposta
- il tempo di lavoro
- ferie e permessi individuali
- l'assenza dal servizio nei casi previsti dalla L. o dai contratti anche collettivi di lavoro
- trasferimenti ad altra sede di lavoro
- procedimenti e provvedimenti disciplinari

questi dati generalmente sono contenuti in atti e documenti prodotti dai lavoratori in sede di assunzione o nel corso del rapporto di lavoro o ancora elaborati da parte del datore di lavoro in pendenza del rapporto di lavoro oppure resi disponibili in albi e bacheche o ancora nelle intranet aziendali.[43]

[43] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.121.

3.3 Il trattamento dei dati

Nel rapporto di lavoro il datore di lavoro inevitabilmente entra in possesso dei dati del lavoratore che può trattare solo ai fini del rapporto stesso. I dati possono essere:

- Indispensabili per la corretta esecuzione del rapporto;
- Indispensabili per attuare previsioni di L., regolamenti, contratti e accordi collettivi.

Il Codice della privacy in materia di protezione dei dati personali prevede che il trattamento dei dati personali avvenga come abbiamo già visto nel paragrafo 2.3 nel rispetto dei principi di:

- Liceità
- Pertinenza
- Trasparenza

Per la spiegazione di questi principi si rimanda al paragrafo 2.3.[44]

[44] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.122.

3.4 Le finalità del trattamento e il consenso

I dati dei singoli lavoratori sono trattabili solo nel caso in cui il fine derivi da un obbligo contrattuale come ad esempio:

- Per verificare l'esatto adempimento della prestazione;
- Per commisurare l'importo della retribuzione, anche per lavoro straordinario, o dei premi da corrispondere;
- Per quantificare le ferie o i permessi;
- Per appurare l'esistenza di una causa legittima di assenza;

Alcuni scopi sono previsti dalla contrattazione collettiva, ad esempio i permessi, i periodi di comporto, altre sono invece previste dalla L., ad esempio le comunicazioni agli enti previdenziali e assistenziali.

Le Linee Guida hanno chiarito tuttavia che in ogni caso lo scopo perseguito dal datore di lavoro per il trattamento dei dati personali non deve essere incompatibile con le finalità per cui sono stati raccolti.

Come detto anche in precedenza i lavoratori devono avere informativa dei dati raccolti ai sensi dell'art.13 del Codice della Privacy.[45]

All'art.23 del Codice viene stabilito che il trattamento dei dati è consentito solo con il consenso espresso che, nel caso in cui riguardasse i dati sensibili, deve essere espresso per iscritto. Il consenso si ritiene validamente prestato nel caso in cui è documentato per iscritto.

All'art.24 vengono stabiliti i casi in cui il consenso non va richiesto ed ai fini del rapporto di lavoro ci interessano i seguenti commi:

- è necessario per adempiere ad un obbligo previsto dalla L., da un regolamento o dalla normativa comunitaria;

[45] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.123.

- è necessario per eseguire gli obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati
- con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;
- riguarda dati contenuti nei curricula, nei casi di cui all’articolo 13, comma 5-bis
- con esclusione della diffusione e fatto salvo quanto previsto dall’articolo 130 del codice, riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell’articolo 2359 del codice civile ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalità amministrativo contabili, come definite all'articolo 34, comma 1-ter, e purché queste finalità siano

previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa di cui all'articolo 13.[46]

È importante sottolineare che in linea di massima il consenso va richiesto se si trattano dati sensibili, tuttavia può non essere richiesto nel caso in cui ai fini dell'adempimento degli obblighi previsti dalla L. o da un regolamento o dalla normativa comunitaria in materia di gestione del rapporto di lavoro previo consenso del Garante. Alla luce di questa considerazione il consenso nel rapporto di lavoro non è necessario quando serve per adempiere ad un obbligo previsto dalla L., da un regolamento o dalla normativa comunitaria.[47]

[46] Art. 24 Codice della Privacy, D.lgs. 196/2003
[47] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.125.

3.5 L’autorizzazione al trattamento dei dati

Ogni anno il Garante della Privacy rilascia un provvedimento generale che autorizza al trattamento dei dati sensibili nei rapporti di lavoro. Il provvedimento n.583 del 11.12.2014 ha validità fino al 31 dicembre 2016 e autorizza il trattamento dei dati sensibili, relativamente al rapporto di lavoro, secondo specifiche prescrizioni.

Il provvedimento stabilisce che i sistemi informativi e programmi informatici devono essere configurati riducendo al minimo l’utilizzazione dei dati personali in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi.

Il trattamento dei dati sensibili deve essere effettuato con operazioni e con modalità specificati nell’autorizzazione. I dati sensibili possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti specificati nell’autorizzazione, ovvero per perseguire le finalità ivi specificate. I dati che, anche a seguito di verifica, risultano eccedenti e non pertinenti non possono essere utilizzati, salvo che per l’eventuale conservazione, a norma di L. dell’atto o del documento che li contiene. I dati sensibili possono essere comunicati, nei limiti pertinenti agli obblighi, agli enti previdenziali assistenziali.[48]

Il lavoratore ha il diritto di avere il controllo dei dati a lui riferibili questo diritto è concretizzato nell’art.7 del d.lgs. n. 196/2003 che per completezza riportiamo:

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:

[48] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.128

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di L., compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Questi diritti devono essere esercitati ai sensi dell’art.8 che prevede una richiesta rivolta al titolare del trattamento senza particolari formalità anche per tramite di un incaricato. Ai commi 2 e 3 dell’art.8 sono previsti i casi in cui la richiesta è esclusa e con riferimento al rapporto di lavoro il comma 4 prevede:

- L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

3.6 Il titolare del trattamento

Il titolare del trattamento, come definito dall'art. 4 lett. f comma 1, è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità alle modalità di trattamento di dati personali. Quando il trattamento dei dati è effettuato da un soggetto giuridico il titolare è rappresentato dalla società stessa, infatti le Linee Guida hanno chiarito che in linea di principio per individuare il titolare del trattamento rileva l'effettivo centro di imputazione del rapporto di lavoro, al di là di quale schema organizzativo sia formalmente adottato dall'azienda come stabilito anche dalla sentenza della corte di cassazione n. 4274 del 24 marzo 2003.

Il problema sorge nel caso in cui si fosse in presenza di aziende con strutture molto articolate, infatti in quel caso risulterebbe molto complicato riuscire ad individuare il titolare del trattamento. In questo caso le Linee Guida suggeriscono di nominare uno o più responsabili del trattamento ai quali deve essere attribuito per iscritto i compiti loro assegnati. In riferimento a questo il Garante ha specificato che "Le società che appartengono a gruppi di imprese individuati in conformità alla L. hanno di regola una distinta ed autonoma titolarità del trattamento in relazione ai dati personali dei propri dipendenti e collaboratori" il titolare del trattamento deve essere in ogni caso conscio del fatto che nominare uno o più responsabili non è sufficiente ad essere esclusi dalla sua eventuale responsabilità. Infatti ai sensi dell'art.15 del D.lgs. n.196/2003, chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 c.c. in tal caso è risarcibile anche il danno non patrimoniale[49].

[49] Cfr R. Schiavone, Controllo *dei Lavoratori*, Op Cit, pp. 130-136.

3.7 Il responsabile e gli incaricati del trattamento

L'art. 4 definisce "responsabile" del trattamento la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati.

Il datore di lavoro deve individuare il responsabile tra i soggetti che per capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, compreso anche il profilo di sicurezza. Il titolare del trattamento può anche nominare più responsabili, prevedendo anche una suddivisione dei compiti. Ovviamente il responsabile dovrà attenersi ai compiti forniti dal titolare e inoltre può essere nominato sia un soggetto interno od esterno all'azienda. Cosi come il titolare anche il responsabile deve fornire informazioni all'interessato in merito ai diritti di cui all'art.7 del codice della privacy e estrarre i documenti nel caso in cui venissero richiesti entro 15 giorni dalla ricezione della domanda. Inoltre il responsabile del trattamento è tenuto al risarcimento dei danni anche non patrimoniali.

Gli "incaricati" del trattamento, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. Quindi possono essere nominati incaricati del trattamento solo le persone fisiche, le quali devono operare sotto la diretta autorità del responsabile o del titolare del trattamento. Gli incaricati devono essere individuati per iscritto individuando gli ambiti del trattamento a cui sono addetti. L'incaricato non deve essere necessariamente un dipendente ma qualsiasi soggetto che cosi come il titolare e il responsabile risponde dei danni commessi anche non patrimoniali.[50]

[50] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, pp.139.140.

3.8 L’amministratore di sistema

L’amministratore di sistema è stato definito con provvedimento del 27.11.2008 dal Garante come quella figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

Sono quei soggetti che risultano concretamente responsabili di specifiche fasi che possono risultare critiche, come ad esempio la fase di salvataggio dei dati quindi di backup e recovery in cui bisogna assicurare l’integrità dei dati e il suo ripristino in caso di problemi alla rete aziendale. Il provvedimento chiarisce le caratteristiche che il soggetto deve possedere per essere nominato amministratore ovvero esperienza capacità ed affidabilità.

È previsto inoltre che la designazione di amministratore di sistema sia individuale e rechi l’indicazione dettagliata degli ambiti di operatività consentiti. Gli estremi identificativi delle persone nominate amministratori di sistema devono essere riportati in un documento interno da mantenere aggiornato e disponibile di accertamento da parte del Garante.

Nel caso in cui il servizio di amministrazione fosse affidato in outsourcing il titolare o il responsabile devono conservare gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema. Inoltre il titolare o responsabile del trattamento deve verificare, con cadenza per lo meno annuale, le tecniche di sicurezza e le misure organizzative riguardanti i trattamenti dei dati personali.[51]

[51] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, pp140-141.

3.9 Le novità del regolamento europeo

Il nuovo regolamento europeo ha portato una serie di modifiche relativamente ad una serie di punti che sono:

1. Il diritto alla portabilità: questo diritto è enunciato all'art.20 del regolamento che prevede la possibilità da parte dell'interessato di poter effettuare la portabilità dei dati. Infatti il soggetto può ricevere in un formato strutturato di uso comune e leggibile a macchina i dati personali che lo riguardano e ha il diritto di trasmetterli ad un altro titolare del trattamento.
2. Data Breach: L'art.33 che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'art.55 entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che non siano presenti rischi effettivi per i dati. Nel caso in cui sia effettuata la comunicazione entro 72 ore, la notifica all'autorità di controllo è corredata da un giustificato motivo.
3. Valutazione d'impatto sulla protezione dei dati: l'art.35 del Regolamento prevede che il titolare del trattamento in caso in cui vengano utilizzate nuove tecnologie possano portare un rischio per i diritti e la libertà delle persone fisiche debba effettuare un'accurata valutazione indicando almeno:
    a. Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
    b. Una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
    c. Una valutazione dei rischi per i diritti e la liberta degli interessati
    d. Le misure previste per affrontare i rischi.

4. Registri delle attività di trattamento: l'art.30 prevede che ogni titolare del trattamento e il suo eventuale rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.
5. Consultazione preventiva: L'art.36 del Regolamento prevede la c.d. consultazione
6. Data protection officer: l'art.37 prevede la designazione del responsabile della protezione dei dati ogniqualvolta il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico oppure nel caso in cui, per natura stessa del trattamento, necessitino di un controllo su larga scala o per categorie particolari di all'art.9 o 10.
7. Certificazione: l'art. 42 e 43 danno ampio spazio alla certificazione degli organismi di certificazione. L'art 42 prevede che gli stati membri incoraggino l'istituzione di meccanismi di certificazione della protezione dei dati allo scopo di dimostrare la conformità al regolamento dei trattamenti effettuati dai responsabili dei trattamenti e dagli incaricati del trattamento.
8. Ambito di applicazione territoriale: l'art.3 del Regolamento sancisce che è da applicare al trattamento dei dati personali effettuati nell'ambito delle attività di uno stabilimento di un responsabile del trattamento di un incaricato del trattamento nell'unione, indipendentemente che sia effettuato o meno nell'unione.
9. Sanzioni: l'art.83 del Regolamento disciplina la materia delle sanzioni che sono appesantite rispetto a quanto previsto e possono arrivare fino al 4% del fatturato mondiale dell'anno precedente di qualsiasi realtà produttiva.[52]

[52] Cfr, M. Iaselli, La privacy per lo studio professionale, pp.15-17.

4. LA VIDEO SORVEGLIANZA E GLI STRUMENTI DI LAVORO

In questo capitolo analizzeremo in dettaglio i controlli più importanti, o comunque più frequenti, con il quale il datore di lavoro potrebbe interfacciarsi. Vedremo inoltre quali sono le disposizioni che fornisce il garante per ogni tipologia di controllo.

4.1 La videosorveglianza ed il controllo degli accessi e delle uscite.

Nonostante il nuovo art. 4 dello S.L non riporti più un espresso divieto nell'uso di impianti audiovisivi e di altre apparecchiature per il controllo a distanza dei lavoratori, tali impianti sono utilizzabili solo nel caso in cui vi siano comprovate esigenze organizzative produttive e/o per la sicurezza sul lavoro e/o per la tutela del patrimonio aziendale. Si può dire quindi che permane comunque il divieto di utilizzo di tali apparecchiature con il fine esclusivo di controllo a distanza dell'attività dei lavoratori.

In pratica è ancora assolutamente vietato:

- Installare impianti allo scopo di controllare l'attività dei dipendenti
- Effettuare controlli occulti celando ai lavoratori i sistemi di sorveglianza.

Alla luce di queste considerazioni si possono ritenere ancora validi l'orientamento espresso a suo tempo dalla sentenza della Cassazione n.1236 del 18/02/1983. In questa sentenza infatti viene proibito il controllo intenzionale e diretto del datore di lavoro in quanto in contrasto con la costituzione e capace di arrecare un danno alla produttività del lavoratore.[53]

Ha chiarito il Garante che non è sufficiente che i lavoratori siano stati informati o che abbiano addirittura acconsentito alla installazione delle telecamere per far venir meno la tutela legislativa e quindi anche il divieto di controllo a distanza.

Rispetto alla norma precedente le novità più importanti sono le seguenti:

[53] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.8

1. Il controllo preterintenzionale del lavoratore è esteso oltre che per i motivi organizzativi, produttivi, di sicurezza sul lavoro anche per la tutela del patrimonio aziendale.
2. In caso di imprese con più entità produttive ubicate in diverse province della stessa regione ovvero in più regioni l'accordo può essere stipulato con le associazioni sindacali più rappresentative sul piano nazionale e in alternativa l'autorizzazione può essere richiesta anziché alla D.T.L al Ministero del Lavoro
3. Viene rafforzato il rispetto della normativa sulla privacy.

In sostanza il nuovo art. 4 dello S.L prevede che, come detto, il controllo preterintenzionale del lavoratore venga ammesso solo se:

L'installazione degli impianti e delle apparecchiature rientri nei casi visti in precedenza ed è comunque necessario che[54]:

- Vi sia un accordo con la RSA o RSU presente in azienda o con quella territoriale;
- L'autorizzazione deve essere richiesta alla DTL competente nel caso in cui il datore di lavoro non abbia raggiunto l'accordo con le RSA o RSU;

Relativamente all'accordo con le RSA o RSU bisogna ricordare che: nel caso sia presente una RSA o una RSU il suo mancato coinvolgimento comporta una condotta antisindacale del datore di lavoro in quanto costituisce un comportamento lesivo di interessi di una larga parte dei lavoratori (Cassazione n.9211 del 16/09/1997). È inoltre da ritenersi ancora valido l'orientamento giurisprudenziale in favore del quale è sufficiente anche un accordo sottoscritto dalla sola maggioranza delle RSA perché la necessaria adesione di tutte le RSA finirebbe per tradursi in un "diritto di veto" utilizzabile anche dalle

[54] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.10

rappresentanze sindacali più esigue (ministero del lavoro risposta ad interpello n. 2975 del 05/12/2005).

In caso di mancato accordo sindacale oppure per le piccole imprese dove non si è costituita sia la RSA sia la RSU è possibile chiedere l'autorizzazione alla direzione territoriale del Lavoro allegando le planimetrie recanti il posizionamento delle telecamere. La D.T.L dopo aver effettuato gli accertamenti previsti emetterà il provvedimento autorizzatorio che di solito contiene le limitazioni previste dalla nota ministeriale n.7162 del 16/04/2012 ovvero stabilisce che:

- Dovrà essere rispettata la disciplina dettata dal Codice in materia di protezione dei dati personali e dai successivi provvedimenti del Garante per la Protezione dei dati Personali, in particolare il provvedimento del 8 aprile 2010;
- Dovrà essere rispettata tutta la normativa in materia di raccolta e conservazione delle immagini;
- Prima della messa in funzione dell'impianto l'azienda dovrà dare apposita informativa scritta al personale dipendente in merito all'attivazione dello stesso, al posizionamento delle telecamere ed alle modalità di funzionamento e dovrà informare i clienti con appositi cartelli;
- L'impianto, che dovrà registrare solo le immagini indispensabili, sarà costituito da telecamere orientate verso le aree maggiormente esposte a rischio di furto e danneggiamento, l'eventuale ripresa di dipendenti avverrà esclusivamente in via incidentale e con criteri di occasionalità;
- All'impianto non potrà essere apportata alcuna modifica e non potrà esser aggiunta alcuna ulteriore apparecchiatura al sistema da installare, se non in conformità al dettato dell'art. 4 della L. 300/70 e previa relativa comunicazione alla DTL competente;

- Le immagini registrate non potranno in nessun caso essere utilizzate per eventuali accertamenti sull'obbligo di diligenza da parte dei lavoratori né per l'adozione di provvedimenti disciplinari (questa prescrizione, ora, non è più possibile per l'autorizzazione rilasciata dopo l'entrata in vigore del nuovo art. 4 S.L. che invece permette l'utilizzo per l'adozione di provvedimenti disciplinari);
- In occasione di ciascun accesso alle immagini l'azienda dovrà darne tempestiva informazione ai lavoratori occupati;
- I lavoratori potranno verificare periodicamente il corretto utilizzo dell'impianto.

Per quanto riguarda gli strumenti di lavoro e quelli per la registrazione degli accessi e delle presenze previsti dal comma 2 dell'art. 4 S.L, bisogna ricordare che attualmente non è più previsto l'obbligo dell'autorizzazione sindacale o amministrativa. Questa possibilità è prevista però solo nel caso in cui lo strumento di lavoro non permetta il controllo preterintenzionale e gli strumenti previsti per la registrazione degli accessi e delle presenze non devono permettere alcun controllo a distanza dei lavoratori.

Fino alla recente modifica legislativa, era generalmente vietato l'utilizzo delle immagini per contestare azioni disciplinari ai dipendenti. Come già ampiamente spiegato in precedenza la norma è stata modificata andandosi ad allineare con il filone giurisprudenziale dei c.d. "controlli difensivi". Infatti l'art. 4 come ora riscritto consente l'utilizzabilità delle immagini rilevate dal sistema di videosorveglianza quale mezzo di prova a sostegno di sanzioni disciplinari.[55] Dello stesso parere è anche il Garante che in un intervento pubblicato sul sito internet, a commento della norma di L., ha sostenuto la stessa tesi. Sarà quindi molto utile redigere un disciplinare interno che preveda in modo chiaro la policy

[55] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.20

prevista per la privacy. A questo fine sarà importante che questo disciplinare sia conforme ai provvedimenti stabiliti dal Garante.

Uno dei recenti provvedimenti in materia di videosorveglianza da parte del Garante può essere sintetizzato come segue:

- È necessario che gli interessati siano informati che stanno accedendo in area videosorvegliata con appostiti cartelli.
- Le immagini vanno conservate al massimo per 24 ore fatto salvo particolari esigenze speciali.
- Solo in alcun casi, per peculiari esigenze tecniche o per la particolare rischiosità dell'attività svolta dal titolare del trattamento, può ritenersi ammesso un tempo più ampio di conservazione dei dati che si ritiene non debba comunque superare la settimana.
- Il sistema impiegato deve essere programmato in modo da cancellare automaticamente le informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.
- Ai lavoratori va fornita informativa nel rispetto dell'art.13 del codice della Privacy.
- Vanno designate per iscritto tutte le persone incaricate del trattamento, autorizzate all'accesso nei locali ove sono situate le postazioni di controllo nonché, nei casi in cui sia indispensabile, a visionare le immagini.

4.2 Il controllo dei dati delle presenze e degli accessi.

È chiaro ed evidente che il datore di lavoro ha il diritto di controllare gli accessi in azienda dei dipendenti ed acquisire i dati che servono per quantificare la prestazione lavorativa.

Nell'ambito di tale attività di controllo, il datore di lavoro, incontra comunque dei limiti posti dal divieto di controllo a distanza dei lavoratori e dalla normativa sulla privacy.

La tecnologia moderna ha portato sensibili miglioramenti nella gestione degli accessi, infatti siamo passati dai registri cartacei al "badge", uno strumento molto veloce e poco invasivo. Tuttavia il badge ha il problema che può essere "passato" anche a terzi non avendo quindi la certezza che il lavoratore che ha timbrato l'ingresso con il badge sia effettivamente a lavoro. Le nuove tecnologie di rilevazione dei dati biometrici (ovvero quei dati che sono ricavati dalle caratteristiche fisiche e comportamentali della singola persona attraverso sistemi automatizzati) forniscono dati più sicuri che consentono di avere certezza dell'accesso effettuato da parte del singolo lavoratore. I dati biometrici sono ad esempio il controllo dell'impronta digitale, il riconoscimento dell'iride, del volto, della voce etc.[56]

Essendo dati strettamente personali, il loro trattamento presenta dei rischi specifici per i diritti e le libertà fondamentali dei lavoratori tutelati dall'art.17 del codice della Privacy. Infatti sull'argomento in questione troviamo limiti posti sia dalle Linee Guida emanate in data 23/11/2006 dalle quali se ne evince che[57]:

- l'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è lecito;

[56] P. Ghini, I. Colombi, *Controllo degli accessi in azienda*, Riviste 24, 2016, p.1
[57] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, pp.52-53

- l’utilizzo di dati biometrici può essere giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui gli stessi sono trattati e, in relazione ai luoghi di lavoro possono essere usati, per presidiare accessi ad “aree sensibili”, tenendo presente la natura delle attività ivi svolte come ad esempio in caso di processi produttivi pericolosi o sottoposti a segreti di varia natura oppure particolari locali destinati alla custodia di beni, documenti segreti o riservati o oggetti di valore;
- nei casi in cui l’uso dei dati biometrici è consentito, la centralizzazione in una banca dati delle informazioni personali trattate nell’ambito di un procedimento di riconoscimento biometrico, risulta di regola sproporzionata e non necessaria;
- in luogo di modalità centralizzate di trattamento dei dati biometrici, deve ritenersi adeguato e sufficiente avvalersi di sistemi efficaci di verifica e di identificazione biometrica basati sulla lettura delle impronte digitali memorizzate su un supporto posto nell’esclusiva disponibilità dell’interessato (una smart card o un dispositivo analogo) e privo di indicazioni nominative riferibili a quest’ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale);
- i dati personali necessari possono essere trattati esclusivamente durante la fase di registrazione;
- per il loro utilizzo e il titolare del trattamento deve raccogliere il preventivo consenso informato degli interessati;
- vanno impartiti agli incaricati apposite istruzioni a cui attenersi, con particolare riguardo al caso di perdita o sottrazione delle carte o dispositivi loro affidati;
- i dati memorizzati devono essere accessibili al personale preposto al rispetto delle misure di sicurezza all’interno dell’impresa, per l’esclusiva

finalità della verifica della loro osservanza, rispettando la disciplina sul controllo a distanza dei lavoratori (art. 4, L. 300/70);

- i dati raccolti non possono essere di regola conservati per un arco di tempo superiore a sette giorni e vanno assicurati, anche quando tale arco temporale possa essere lecitamente protratto, idonei meccanismi di cancellazione automatica dei dati;
- per fattispecie particolari o in ragione di situazioni eccezionali non considerate nelle Linee Guida, i titolari del trattamento devono presentare apposito interpello al Garante, ai sensi dell'art. 17 del Codice per la Privacy.

Successivamente il Garante, in data 12/11/2014, ha emesso un "provvedimento generale descrittivo in materia di biometria" in cui impone degli obblighi più dettagliati e più specifici contenuti nello specifico Allegato B il quale impone l'obbligo del "data breach" ovvero il titolare del trattamento che pone in essere trattamenti di natura Biometrica deve ottemperare ad un ulteriore incombenza nel caso in cui avvengono dei fatti che abbiano comportato la violazione di questi dati ultra sensibili.

Quest'allegato infatti precisa che la violazione debba essere messa a conoscenza dell'Autorità Garante. All'interno dell'allegato il Garante ha inserito un modello per effettuare questa comunicazione in cui il titolare del trattamento dovrà riportare ogni informazione utile atta a indicare con la maggiore accuratezza possibile i dati che sono stati oggetto di tali violazioni, la tipologia di violazione accaduta, il dispositivo oggetto della violazione. Questa misura del "data breach" come abbiamo visto nel paragrafo 3.9 viene riproposta anche nel regolamento europeo di recente emanazione.[58]

[58] P. Ghini, I. Colombi, *Controllo degli accessi in azienda*, Op Cit, p.3

I dati biometrici lasciano, al datore di lavoro, un margine di incertezza in quanto sono dati ultrasensibili e abbiamo visto che il Garante pone regole molto dure relativamente ai rischi in caso di perdita dei dati. Allora la domanda che ci poniamo è la seguente: può in qualche modo il datore di lavoro difendersi nel caso in cui ci sia un utilizzo fraudolento del badge? In risposta a questo quesito la giurisprudenza ha recentemente affermato che l'utilizzo delle videocamere in caso di verifica di un reato, installate a seguito indizi gravi precisi e concordanti, sono sempre ammessi. Questo è l'orientamento ribadito dalla recentissima sentenza della corte di cassazione del 01/08/2016 n.33567 che ha rafforzato il principio che le garanzie procedurali previste dall'art. 4 S.L, secondo comma, dello statuto dei lavoratori non trovano applicazione quando si procede all'accertamento di fatti che costituiscono reato.[59]

[59] D. Alberici, "*Videoriprese anti-fannulloni*", Italia oggi, 02/08/2016, p.27

4.3 Il controllo del traffico telefonico

Il nuovo testo dell'art. 4 S.L non richiede alcun accordo per il controllo del traffico telefonico, in quanto il telefono è uno strumento per rendere la prestazione lavorativa. Di conseguenza è richiesto che il datore di lavoro fornisca adeguata informativa sulle modalità d'uso e sulle possibilità di effettuare i controlli in merito. Le informazioni raccolte sono utilizzabili anche ai fini sanzionatori. È chiaro ed evidente che il contenuto della conversazione telefonica è costituzionalmente tutelato dall'art.15 infatti ascoltare o registrare le conversazioni è vietato dal codice penale.

Il ministero del lavoro con risposta due interpelli ha chiarito che solo nel caso i controlli siano effettuati a campione e né il lavoratore né gli altri soggetti coinvolti siano identificabili solo in questo caso non sussiste il reato e nemmeno la violazione della privacy.

Già da molto tempo si è cominciato a ritenere importante per il datore di lavoro la possibilità di verificare che i dipendenti non abusino del telefono aziendale. Infatti già dagli anni 90 la giurisprudenza ha costantemente concordato sulla legittimità del licenziamento del dipendente che utilizzi il telefono aziendale per fini personali e sulla liceità dei controlli diretti a verificare il corretto utilizzo del telefono aziendale ovviamente senza che il controllo si trasformi in un controllo dell'attività lavorativa. La sentenza n. 4746 del 0.3.04.2002 aveva affermato che l'abuso del telefono aziendale costituisse giustificato motivo di licenziamento indipendentemente dall'entità del danno creato al datore di lavoro.[60]

Per difendere i propri interessi, il datore di lavoro, può inserire nel codice disciplinare il divieto per i lavoratori di effettuare telefonate personali prevedendo anche la sanzione espulsiva in caso di reiterate violazioni.

[60] Cfr, R. Schiavone, *Controllo dei Lavoratori*, Op Cit, p.43

Chiaramente non è possibile prevedere un divieto assoluto di effettuare telefonate personali per cui è consigliabile ammetterle per necessità impellenti. A tal proposito la sentenza n. 10062 del 10.07.2002, ha affermato che la continua reiterazione di una condotta vietata dal codice disciplinare fa venire meno la fiducia di lavoro nei confronti del proprio dipendenti. Tuttavia in passato accadeva che, per evitare di violare la privacy del dipendente, si suggeriva al datore di lavoro di farsi firmare il consenso ad effettuare verifiche, adesso invece è sufficiente un'adeguata informativa sulla modalità e sulla possibilità di effettuare controlli in merito nel rispetto del codice della privacy. Le informazioni così raccolte saranno sicuramente utilizzabili anche ai fini sanzionatori.

È ammissibile inoltre sanzionare il lavoratore nel caso in cui non abbia vigilato sul telefono assegnatogli creando un danno all'azienda. La Corte di Cassazione ha infatti ritenuto, con sentenza n. 15534 del 09.07.2007, lecita la sanzione espulsiva in quanto il telefono aziendale era stato utilizzato in maniera illecita da parte di un terzo.[61]

Terminiamo facendo riferimento alle apparecchiature che sono finalizzate ad effettuare un controllo dei costi del servizio telefonico, nonché una più corretta e puntuale imputazione contabile di tali costi alle singole unità organizzative, il ministero del Lavoro, con risposta all'interpello n.218 del 06.06.2006 ha chiarito che:

- l'imputazione contabile dei costi telefonici al centro di costo nel suo complesso, non permette neanche incidentalmente il controllo dell'attività dei lavoratori, per cui tale fattispecie non rientra nella procedura di cui al comma 2 (adesso comma 1), art. 4, L. 300/70, ovvero necessità di accordo/autorizzazione;

[61] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.44

- qualora l’imputazione contabile sia effettuata nei confronti della singola utenza, occorre verificare caso per caso se tale operazione consenta un controllo indiretto sull’attività lavorativa dei dipendenti.

Quanto sopra, letto alla luce del nuovo art. 4 S.L, ci permette di affermare che il primo punto rimane uguale, mentre nel secondo caso entra in gioco la c.d. “policy aziendale” la quale dovrà assicurare che non vi è controllo indiretto sull’attività lavorativa dei dipendenti.

4.4 La dotazione di smartphone.

Lo smartphone è il classico strumento di lavoro grazie al quale è possibile anche localizzare geograficamente i lavoratori mediante un'apposita applicazione. Ovviamente la localizzazione non può avere mera finalità di controllo a distanza ma deve essere giustificato dalle esigenze previste dall'art. 4 S.L.

Trattandosi di uno strumento di lavoro, di cui il dipendente può fare anche un uso personale, le modalità previste dal Garante a tutela della riservatezza sono importanti e sono previste dai provvedimenti n.401 e 448 del 2014. In particolare viene previsto che[62]:

- Dovranno essere adottate specifiche misure volte a garantire che le informazioni, visibili o utilizzabili dalla "app", siano solo quelle di geo localizzazione, impedendo l'accesso ad altri dati, quali ad esempio, sms, posta elettronica, traffico telefonico;
- Il sistema deve essere configurato in modo tale che sullo schermo dello smartphone compaia sempre, ben visibile, un'icona che indichi ai dipendenti che la funzione localizzazione è attiva;
- I lavoratori dovranno essere informati sulle caratteristiche dell'applicazione, compresi i tempi e le modalità di attivazione, nonché sui trattamenti di dati effettuati dalle società;
- Per rispettare i principi di necessità, pertinenza e non eccedenza la rilevazione dei dati di geo localizzazione non deve essere continuativa, ma avvenire ad intervalli stabiliti;
- L'ultima rilevazione deve cancellare quella precedente;
- Prima di attivare il sistema i datori devono notificare al Garante il trattamento di dati sulla localizzazione.

[62] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.49

4.5 La navigazione in internet ed il controllo dei dischi fissi e dei PC aziendali.

Il datore di lavoro può avere la volontà di controllare la regolarità degli accessi ad internet del lavoratore utilizzando programmi informatici. Tuttavia, stante l'art. 4 dello S.L anche dopo la modifica prevista dal D.lgs. 151/2015 è vietato utilizzare programmi in grado di monitorare esclusivamente la prestazione lavorativa ed è invece ammesso l'utilizzo di programmi che abbiano altre finalità riconosciute lecite e cioè che abbiano finalità organizzative, produttive e per la tutela del patrimonio aziendale e che, solo incidentalmente, permettano anche il controllo della navigazione dei dipendenti.

Comunque per usare questi programmi è necessario o l'accordo con le RSA/RSU oppure l'autorizzazione della DTL.

Il Garante in merito alla navigazione ha emanato le Linee Guida del 01/03/2007 suggerendo di pubblicizzare adeguatamente un disciplinare interno in cui è opportuno specificare:[63]

- quali comportamenti siano o meno tollerati rispetto alla "navigazione" in Internet (ad es., il download di software o di • le musicali), oppure alla tenuta di • le nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di rete, anche solo da determinate postazioni di lavoro, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di • le di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;

[63] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, pp.58-59

- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di • le di log);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla L., anche saltuari o occasionali, indicando le ragioni legittime, speci• che e non generiche, per cui verrebbero effettuati (anche per veri• che sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la rete Internet sia utilizzata indebitamente;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute speci• che • gure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi.

È evidente che il controllo degli accessi in internet e il controllo dei dischi fissi è molto delicato in quanto può incidere sui diritti costituzionali dei lavoratori come già considerato nel paragrafo 2.2.

In ogni caso anche sulla base delle ragioni di tutela del patrimonio aziendale, previo accordo sindacale o con autorizzazione della D.T.L , è consentito al datore di lavoro di controllare con programmi specifici gli accessi internet ed i dischi fissi del lavoratore.

4.6 Le Schede Sim dei PC

Un sistema che può permettere di effettuare un controllo a distanza dei dipendenti è l'inserimento di una SIM nel personal computer aziendale. Infatti l'inserimento della SIM nel PC aziendale è potenzialmente utilizzabile in tal senso in quanto consente al datore di lavoro di conoscere l'attività e gli spostamenti di ogni lavoratore. Quindi la consegna del personal computer sprovvisto di SIM non è soggetta ad accordo o autorizzazione ma l'inserimento della SIM fa diventare necessario l'accordo.

A conferma della necessità dell'accordo si può ricordare la risposta del Ministero del Lavoro prot. 6585 del 28/11/2006 all'interpello di una azienda farmaceutica che aveva dotato gli informatori scientifici di personal computer muniti di un programma che inviava al server aziendale la registrazione di data e ora delle visite effettuate, ed inoltre con l'inserimento di una scheda SIM l'azienda poteva verificare gli spostamenti del dipendente.

Il ministero nel caso di specie ha ritenuto necessario l'accordo sindacale o l'autorizzazione della DTL. Si ritiene che quanto considerato nella risposta all'interpello sia valida anche in applicazione del nuovo art. 4 S.L.[64]

[64] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, pp.64-65

4.7 La posta elettronica

Un altro controllo molto delicato è quello riguardante la posta elettronica. Ovvero la possibilità da parte del datore di lavoro di andare a controllare la posta elettronica messa a disposizione del lavoratore.

Affrontando questo strumento di lavoro bisogna tenere conto di quanto previsto dall'art.616 del codice penale e tenere ben presente i casi in cui la corrispondenza è considerata "chiusa".

La corte di cassazione con la sentenza n.47096 del 11-19 dicembre 2007 ha chiarito che: "posta l'indiscussa estensione dell'art 616 del codice penale deve tuttavia ritenersi che la corrispondenza elettronica possa essere qualificata come "chiusa" solo nei confronti dei soggetti che non siano legittimati all'accesso ai sistemi informatici di invio o ricezione dei singoli messaggi. Infatti diversamente da quanto avviene per la corrispondenza cartacea, di regola accessibile solo al destinatario, è appunto la legittimazione all'uso del sistema informatico o telematico che abilita alla conoscenza delle informazioni in esso custodite. Sicché tale legittimazione può dipendere non solo dalla proprietà, ma soprattutto dalle norme che regolano l'uso degli impianti. E quando in particolare il sistema telematico sia protetto da una password, deve ritenersi che la corrispondenza in esso custodita sia lecitamente conoscibile da parte di tutti coloro che legittimamente dispongano della chiave informatica di accesso. Anche quando la legittimazione all'accesso sia condizionata, l'eventuale violazione di tali condizioni può rilevare sotto altri profili, ma non può valere a qualificare la corrispondenza come "chiusa" anche nei confronti di chi sin dall'origine abbia un ordinario titolo di accesso."[65]

Quindi il principio di diritto che viene affermato è il seguente:

[65] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, p.69

- per chi non è un superiore gerarchico legittimato all'accesso dei sistemi informatici la corrispondenza informatica è da considerarsi "chiusa" con applicazione dell'art.616 c.p.
- per chi è legittimato la corrispondenza informatica è conoscibile nel rispetto della privacy e quindi delle Linee Guida del 01/03/2007 e della policy aziendale.

La policy aziendale, da pubblicizzare adeguatamente, deve contenere[66]:

- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica, anche solo da determinate caselle oppure ricorrendo a sistemi di web mail, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla L., anche saltuari o occasionali, indicando le ragioni legittime per cui verrebbero effettuati e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica sia utilizzata indebitamente;
- le soluzioni pre• gurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti.

[66] R. Schiavone, Controllo *dei Lavoratori*, Op Cit., P.70

In commercio esistono programmi informatici che hanno il fine di monitorare la posta elettronica ed altri programmi che la monitorano solo incidentalmente. La prima tipologia di programma rientra fra quelle vietate anche sulla base dell'art. 4 modificato. La seconda tipologia è ammessa previo accordo o autorizzazione.

Secondo il Garante l'utilizzo dei programmi che incidentalmente monitorano la posta elettronica può avvenire nel rispetto dei seguenti suggerimenti che sono dati al fine di evitare che il datore di lavoro sconfini in un controllo non ammessi:

- si deve valutare attentamente l'impatto sui diritti dei lavoratori prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento dei dati;
- Vanno preventivamente individuati, anche solo per tipologie, i lavoratori a cui è accordato l'utilizzo della posta elettronica;
- Va determinata l'ubicazione riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo;
- Vanno adottate tutte le misure tecnologiche volte a minimizzare l'uso di dati identi• cativi (c.d. privacy enhancing technologies – PETs);
- Con riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa. La mancata esplicitazione di una policy può determinare anche una legittima aspettativa del lavoratore, o di terzi, di con• denzialità rispetto ad alcune forme di comunicazione. É quindi opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Per questo è opportuno che:

• il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, uf• ciovendite@ente.it, uf• cioreclami@società.com, urp@ ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente. it, rossi@società.com, mario.rossi@società.it);

• il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;

• il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É opportuno anche prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi web mail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;

• in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (• duciario) a veri• care il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo

svolgimento dell’attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;

• i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l’eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell’organizzazione di appartenenza del mittente e con eventuale rinvio alla policy datoriale;

- I sistemi vanno programmati e con• gurati in modo da cancellare periodicamente ed automaticamente i dati relativi al traffico telematico, la cui conservazione non sia necessaria.

4.8 La scatola nera (black box) sui veicoli aziendali.

La scatola nera è un sistema automatizzato montato sugli automezzi che permette di ottenere informazioni omogenee, a supporto dell'organizzazione aziendale, finalizzate a pianificare e ottimizzare la gestione delle flotte aziendali.

Inoltre la scatola nera assicura le esigenze di sicurezza sul lavoro in quanto:

- Monitora la scadenza degli interventi di manutenzione dei veicoli e permette, quindi, una programmazione della stessa;
- a seguito di incidente, attiva in tempo reale ed automaticamente una "chiamata di emergenza" ad una sala operativa esterna alla società che consente un intervento tempestivo per soccorrere l'autista e chi, eventualmente, lo accompagna;
- Consente di ricostruire le dinamiche degli eventuali incidenti, anche ai • ni assicurativi, ed offre un valido supporto in caso di controversie legali;
- È un deterrente contro i furti dei veicoli, assicurando in tal senso non solo la sicurezza del veicolo stesso ma anche quella degli effetti trasportati.

In più l'utilizzo della scatola nera consente anche una sensibile riduzione del premio della polizza auto. Si tratta comunque di uno strumento di lavoro che può essere installato perché necessario per le esigenze organizzative, produttive, di sicurezza sul lavoro e del patrimonio aziendale però poiché lo strumento consente anche un controllo dell'attività del lavoratore i datori di lavoro devono raggiungere l'accordo RSU/RSA oppure ottenere l'autorizzazione DTL. È come sempre obbligatorio fornire un'adeguata informativa ai lavoratori ed è raccomandata una chiara policy aziendale.[67]

Relativamente alla back box il ministero del lavoro ha diramato una nota con prot. 8537 del 07.05.2012 a tutte le DTL indicando quali sono le condizioni

[67] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, P.73

affinché l'autorizzazione possa essere rilasciata, la nota in sintesi prevede le seguenti condizioni[68]:

- L'azienda dovrà dare apposita informativa scritta al personale dipendente in merito alle modalità di funzionamento e alle • nalità che giustificano la relativa autorizzazione;
- All'impianto non potrà essere apportata alcuna modifica e non potrà essere aggiunta alcuna ulteriore apparecchiatura al sistema da installare se non in conformità al dettato dell'art. 4 della L. 300/1970;
- I dati scaricati dai dispositivi installati a bordo dei veicoli devono essere raggruppati dal fornitore e resi disponibili alla società datrice di lavoro in forma aggregata. È fatto esplicito divieto all'azienda di richiedere acquisire ed utilizzare dati non in forma aggregata, in modo da escludere che si possa risalire a singole prestazioni;
- Le informazioni non potranno in nessun caso essere utilizzate per eventuali accertamenti sul l'obbligo di diligenza da parte dei lavoratori né per l'adozione di eventuali provvedimenti disciplinari (questa condizione non è più valida dopo l'entrata in vigore del nuovo art. 4 S.L);
- Essendo la raccolta dei dati esclusivamente destinata alle esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, e di protezione del patrimonio aziendale rimane esclusa ogni altra • nalità, diretta e indiretta, di controllo a distanza dell'attività lavorativa dei dipendenti;
- dovrà essere rispettata tutta la normativa in materia di raccolta e conservazione delle immagini.

[68] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, P.74

4.9 La radio frequency identification (RFID)

La tecnologia RFID è basata sull'invio di onde radio per consentire l'identificazione di oggetti cui è stata apposta un'etichetta elettronica in grado di essere letta da un apposito lettore.

Il lettore, interagendo con l'etichetta, ottiene informazioni che vengono gestite da un software. Il sistema RFID viene utilizzato anche nell'ambito di rapporti di lavoro in riferimento alla possibilità di controllare gli ingressi principali alle aree riservate o alle aree in cui va garantita la sicurezza.

Le etichette di solito sono inserite nelle schede magnetiche ovvero il "badge" dei dipendenti. Il sistema RFID se impiegato per monitorare gli ingressi rientra nella casistica di cui al secondo comma dell'art. 4 S.L e quindi si stratta di strumenti che sono utilizzabili dal datore di lavoro senza bisogno di un accordo sindacale a condizione di aver rilasciato un'adeguata informativa.

È importante che l'utilizzo del RFID non sconfini in un controllo dell'attività del lavoratore. Per questo il Garante ha prescritto alcune misure di tutela che con riferimento al rapporto di lavoro sono le seguenti:

- la necessità di rispettare, nell'utilizzo di tali tecniche, oltre che il Codice della Privacy, anche il divieto di controllo a distanza del lavoratore (art. 4 L. 300/70 ; art. 114 del Codice);
- che, nei casi di impiego di RFID per la veri• ca di accessi a determinati luoghi riservati devono essere predisposte idonee cautele per i diritti e le libertà degli interessati. In particolare, nel caso in cui si intenda utilizzare tali tecniche per veri• care accessi a luoghi di lavoro, o comunque sul luogo di lavoro, va tenuto conto che lo Statuto dei lavoratori vieta l'uso di impianti e apparecchiature per • nalità di controllo a distanza dell'attività dei lavoratori e, nel caso in cui il loro impiego risulti necessario per altre • nalità, prescrive alcune garanzie (art. 4 L. 20 maggio 1970, n. 300; art.

114 del Codice) alle quali si affianca l'osservanza dei principi di necessità, • nalità e proporzionalità del trattamento dei dati.

Per il sistema RFID inserito nel "badge":

- i lavoratori siano stati informati sulle modalità di funzionamento del sistema;
- vengano raccolti esclusivamente i dati relativi all'entrata o all'uscita del lavoratore attraverso l'accostamento del badge al lettore, il quale deve segnalare, in modo evidente, la registrazione dei dati medesimi ed evitare pertanto la raccolta di dati all'insaputa del prestatore di lavoro. Un tale sistema non risulta, infatti, raccogliere dati personali eccedenti rispetto alle • nalità di gestione del rapporto di lavoro.[69]

[69] Cfr. R. Schiavone, Controllo *dei Lavoratori*, Op Cit, pp.77-79

4.10 I sistemi GPS

I GPS o localizzatori satellitari permettono il controllo dei lavoratori che per svolgere la loro prestazione lavorativa si spostano a bordo di veicoli.

Questi sistemi permettono di controllare gli spostamenti dei dipendenti i tempi di percorrenza e per questo si è ritenuto che rientrassero nei sistemi di controllo dell'art. 4 e quindi utilizzabili previo accordo o autorizzazione.

È da ritenere che anche alla luce del nuovo art. 4 dello S.L l'installazione del GPS sia possibile effettuarlo solo previo accordo o autorizzazione.

Infatti fino ad ora le D.T.L rilasciavano l'autorizzazione all'installazione del GPS a condizione che sia lasciata al lavoratore la possibilità di azionare o staccare volontariamente il rilevamento satellitare.

Alla luce di quanto previsto dal nuovo art. 4 dello S.L tale richiesta non pare giustificabile perché fra i motivi che giustificano il controllo c'è anche la tutela del patrimonio aziendale e quindi un'azienda potrebbe anche pretendere che il rilevamento satellitare non possa essere volontariamente disattivato dal lavoratore perché così facendo si potrebbe mettere a rischio il bene aziendale.

In merito all'installazione del GPS è da tenere presente che il Garante ha dato le seguenti raccomandazioni:[70]

- quale misura necessaria, per il rispetto del principio di necessità, che la posizione del veicolo non sia di regola monitorata continuativamente dal titolare del trattamento, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite;
- quale misura necessaria, in base al principio di pertinenza e non eccedenza, e quindi che i tempi di conservazione delle diverse tipologie di

[70] R. Schiavone, Controllo *dei Lavoratori*, Op Cit, pp. 84-85

dati personali eventualmente trattati siano commisurati tenendo conto di ciascuna delle • nalità in concreto perseguite;

- quale misura necessaria, la designazione quali responsabili del trattamento degli operatori economici che forniscono i servizi di localizzazione del veicolo e di trasmissione della posizione del medesimo, impartendo loro le necessarie istruzioni in ordine all'utilizzo legittimo dei dati raccolti per le sole • nalità previste dall'accordo che regola la fornitura del servizio di localizzazione, con la determinazione delle tipologie di dati da trattare nonché delle modalità e dei tempi della loro eventuale conservazione;
- quale misura opportuna, un modello sempli• cato di informativa, al • ne di rendere noto agli interessati il trattamento effettuato mediante il sistema di localizzazione del veicolo.

Inoltre il Garante relativamente ai GPS installati da un'azienda di telefonia ne ha consentito il seguente uso:[71]

- Localizzare il veicolo su una mappa cartogra• ca in tempo reale;
- Verificare il tragitto percorso;
- Verificare gli orari delle soste effettuate ed i tempi di guida;
- Calcolare la velocità ed i chilometri percorsi;
- Controllare gli eventi veri• catisi lungo il percorso (soste e spostamenti in orari non previsti, arrivo in aree predeterminate, ecc.);
- Comunicare costantemente con il conducente;
- Gestire i punti di interesse (indirizzi della clientela, magazzini, impianti, ecc.) con possibilità di veri• care le soste effettuate ed i tempi di fermata;
- Gestire la manutenzione ordinaria del veicolo;

Disponendo che l'azienda desse l'informativa preventiva a tutti gli autisti e seguendo la procedura di accordo o autorizzazione.

[71] R. Schiavone, Controllo *dei Lavoratori*, Op Citp.86

Sulla questione del GPS tuttavia la questione delicata è capire in quali casi si tratta di uno strumento di lavoro oppure di uno strumento che risponde ad esigenze organizzative o di sicurezza. Infatti a seconda della categoria, comporta o meno la richiesta di autorizzazione o l'instaurazione di un accordo sindacale.

In merito a questa domanda si ha una recente risposta della DTL di Milano che ha preso una posizione al riguardo. Infatti ha enunciato che l'automezzo dato al lavoratore in uso promiscuo al dipendente è certamente strumento di lavoro e lo è nella sua unicità. Inoltre ha anche affermato che il sistema GPS non è da considerare separatamente anche nel caso in cui venisse installato successivamente. Questa posizione è sicuramente in linea con la ratio della nuova norma tuttavia non è chiaro se sarà condivisa dal ministero. Infatti sul sito internet del ministero il modulo per richiedere l'autorizzazione all'installazione di strumenti di controllo, rientranti nel primo comma della norma, mette sullo stesso piano telecamere e apparecchiature GPS.[72]

[72] A. Bottini, "Valutazioni differenti sulla << natura>> del Gps", *Il sole 24 ore,* 24 agosto 2016, p.28

4.11 Lo Smart Working ed i controlli possibili.

Lo Smart Working ovvero il "lavoro agile" è un ripensamento intelligente delle modalità lavorative derivante dalle nuove tecnologie informatiche che consentono il lavoro anche fuori dalle aziende nonché tramite la condivisione delle prestazioni di lavoro superando la rigidità degli orari di lavoro. Questo permette alle aziende rendendo il lavoro più flessibile.[73]

Si tratta di un modo di pensare il lavoro che per almeno il 40% delle situazioni risulta essere migliorativo della produttività e delle condizioni di lavoro.

Lo Smart Working non è solo consentire alle persone di lavorare uno o due giorni alla settimana da casa ma è una nuova filosofia manageriale che richiede di instaurare tra persone un rapporto maturo basato sulla fiducia, sull'impegno al risultato, sulla disponibilità a mettersi in discussione. Tutto questo avvalendosi delle tecnologie.[74]

Attualmente ci sono due progetti di L. che intendono agevolare e incentivare lo "Smart Working" e ovviamente si porranno in evidenza anche i problemi del controllo a distanza del lavoratore e del necessario punto di equilibrio fra esigenze di controllo del datore di lavoro e la privacy del lavoratore.

Il disegno di L. AS2233 per il lavoro agile in merito al potere di controllo e disciplinare all'art.16 e 17 dispone:[75]

- L'accordo relativo alla modalità 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 L. 300/70, e successive modificazioni.

[73] M. Corso, F. Crespi, A.C. Scacco, *Smart Working*, Il sole24ore, 2016, p.12
[74] M. Corso, F. Crespi, A.C. Scacco, *Smart Working*, Op cit. p.8
[75] M. Corso, F. Crespi, A.C. Scacco, *Smart Working*, Op cit. pp.123-129

- 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.
- Il datore di lavoro deve adottare misure atte a garantire la protezione dei dati utilizzati ed elaborati dal lavoratore che svolge la prestazione lavorativa in modalità di lavoro agile.
- Il lavoratore è tenuto a custodire con diligenza gli strumenti tecnologici messi a disposizione dal datore di lavoro ed è responsabile della riservatezza dei dati cui può accedere tramite l’uso di tali strumenti.

È evidente che il Legislatore delega all’accordo fra le parti la disciplina del lavoro agile ed il contemperamento degli apposti interessi nel rispetto dell’art. 4 della L. 300/70. Non è prevista la possibilità di richiesta di autorizzazione alla DTL.

Per quanto riguarda la custodia e riservatezza dei dati viene confermato l’obbligo del datore di lavoro di garantire la protezione dei dati e l’obbligo di riservatezza del lavoratore rispetto ai dati di cui viene messo a conoscenza nel suo lavoro mediante gli strumenti di lavoro assegnati.

Un esempio di decalogo “privacy” nel lavoro agile è previsto nel contratto aziendale CARIPARMA che dispone quanto segue:

1. le conversazioni tra Dipendente e altri Interessati non devono essere oggetto di ascolto da parte di soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di proteggere la confidenzialità; pertanto occorre:
    a. evitare di effettuare colloqui ad alta voce, di persona o per telefono, in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione; - accertarsi che il coniuge o eventuali parenti o

conoscenti non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti l'attività lavorativa;

b. non utilizzare familiari o terzi per veicolare informazioni, anche se ritenute "banali", afferenti l'attività lavorativa;
c. nel caso di conversazioni telefoniche instaurate a seguito di chiamate inoltrate o ricevute, accertare, con cura, che l'interlocutore sia effettivamente il Cliente/Collega/Fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione;

2. i dati personali propri o di altri Interessati non devono essere annotati su fogli di carta o file provvisori, bensì occorre utilizzare le modulistiche e le procedure aziendali;

3. prestare particolare attenzione quando si trasportano da un locale all'altro, da uno stabile all'altro, da un luogo ad un altro (mediante mezzi pubblici o privati o anche a piedi) documenti contenenti dati personali; in tal senso, è utile evitare di interrompere il tragitto con conversazioni non necessarie o con soste i luoghi non idonei (ad es. bar, mense, negozi, edicole, ecc.); è vietato lasciare in locali pubblici o aperti al pubblico (anche temporaneamente) la corrispondenza e/o qualsiasi documentazione aziendale; in caso di trasmissione di dati personali via fax, accertarsi che il destinatario del fax sia pronto a riceverli immediatamente (affinché i documenti trasmessi non rimangano incustoditi presso la macchina);

4. evitare di duplicare gli archivi già presenti nei locali della sede dell'unità organizzativa di appartenenza. In ogni caso, la creazione di un archivio fuori dai locali aziendali è possibile solo, in via temporanea, per rispondere a necessità straordinarie e contingenti. Il contenuto di tali archivi provvisori deve essere inventariato e condiviso con il Responsabile gerarchico; la

fotoriproduzione di documentazione cartacea contenente dati personali deve avvenire solo se strettamente necessaria, facendo attenzione a non lasciare gli originali e/o le copie nelle fotocopiatrici e a che le riproduzioni siano prelevate immediatamente dalla stampante (onde evitare la consultazione degli stessi da parte di persone non autorizzate).

5. per quanto riguarda la generica conservazione dei dati personali utilizzati dal dipendente in "Lavoro agile", il Responsabile dell'unità organizzativa deve adottare soluzioni organizzative idonee a ridurre al minimo i rischi di distruzione, perdita, accessi non consentiti ai dati.

6. Più in dettaglio, per quanto concerne l'utilizzo di documenti cartacei contenenti dati personali e prelevati dagli archivi aziendali, si sottolinea che il trasferimento dei dati personali all'esterno della Società del Gruppo deve essere giustificato da necessità strettamente correlate all'esercizio dell'attività lavorativa, agli obblighi di L. o alla difesa dell'interesse del Gruppo. La circolazione dei dati personali cartacei, in situazione di mobilità, deve essere ridotta al minimo indispensabile i dati devono essere raccolti in porta documenti riportanti l'identificazione del Dipendente utilizzatore e il suo recapito telefonico. In particolare, i documenti cartacei:

a. devono essere utilizzati solo per il tempo necessario allo svolgimento dei compiti assegnati e poi riportati negli archivi aziendali dedicati alla loro conservazione;
b. non devono essere lasciati incustoditi; pertanto, nel caso di assenza, anche momentanea, dal luogo in cui si svolge il "Lavoro Agile" è necessario chiudere a chiave i locali che ospitano i dati ovvero riporli dentro un armadio/cassetto chiuso a chiave; non devono restare, senza ragione, applicati su supporti (lavagne o simili) che possano essere visionati da persone non autorizzate;

c. devono essere resi illeggibili prima di essere cestinati, qualora siano destinati a divenire rifiuti, (ad es. strappando più volte la carta in modo che i contenuti diventino non decifrabili/non ricostruibili).

7. i file devono essere salvati su un disco di rete ad accesso riservato a personale autorizzato, non devono - salvo casi limitati e motivati da esigenze di servizio e comunque autorizzati dal Responsabile di struttura -essere memorizzati in modo permanente sull'hard disk del computer in dotazione; i dati non devono, se non strettamente necessario, essere memorizzati su supporti rimovibili.

8. la password di accesso deve essere conservata con diligenza in modo che resti riservata, evitando, sotto la responsabilità del Dipendente, che altri ne vengano a conoscenza;

9. il computer ed eventuali altri strumenti in dotazione (tablet, smartphone ecc.), non devono essere lasciati incustoditi ed accessibili a persone non autorizzate (in caso di allontanamento, anche temporaneo, dalla postazione di lavoro il Dipendente è tenuto a disconnettere la sessione di lavoro bloccando l'operatività del computer.

La lettura del precedente accordo rende l'idea delle diverse problematiche inerenti il "lavoro agile" e chi scrive ritiene che sarebbe opportuno anche prevedere le sanzioni applicate in caso di mancato rispetto dell'accordo.

È evidente che, trattandosi di una banca, l'importanza della privacy è determinante e quindi l'attenzione alla privacy è molto alta e densa di adempimenti e casi particolari. Comunque anche per molte altre attività imprenditoriali (ad esempio chimica- farmaceutica) che professionali le problematiche da tenere presente sono molto simili.

Infatti immaginiamo il “lavoro Agile” in uno studio professionale dove la necessità di tutelare la privacy dei clienti è forte. In questo caso vediamo subito il problema di dover regolare il caso in cui il dipendente porta i “fascicoli cartacei a casa”. Una chiara e applicabile “policy aziendale” sulla privacy è così necessaria che non si può nemmeno iniziare a pensare al “lavoro agile” se non si affrontano i problemi di privacy del lavoratore e quelli dei terzi.

5.CONCLUSIONI

Al termine di questo lavoro siamo arrivati al punto in cui dobbiamo cercare di trarre delle conclusioni sull'argomento trattato. Sicuramente le conclusioni, se intese come risposte a domande, non sono molte in quanto il tema ha molte questioni su cui non è semplice dare risposte certe. In ogni modo cercheremo di elencare quali sono le principali novità e le problematiche che rimangono aperte.

Sicuramente il fine della modifica è quello di andare a "tappare" delle falle che erano presenti nel precedente articolo e che avevano lasciato domande aperte a cui il legislatore, negli anni a venire, non aveva fornito risposte e che pertanto avevano portato a correttivi di tipo giurisprudenziale come ad esempio i controlli difensivi.

L'interpretazione del nuovo art. 4 dello S.L porta a concludere che relativamente al comma 1 è stata resa la norma in senso positivo anziché negativo, ma le condizioni per legittimare il controllo sono rimaste di fatto le stesse con l'importante inclusione della tutela del patrimonio aziendale. Anzi l'intervento di riforma includendo il patrimonio aziendale porta a rivedere e ridurre l'ambito dei "controlli difensivi" di creazione giurisprudenziale.

A questo punto sembrerebbero rimanere al di fuori dell'art. 4 dello S.L solo quei controlli difensivi estranei al rapporto di lavoro, posti in essere con modalità tali da escludere qualsiasi potenzialità di controllo della prestazione lavorativa e quindi non sottoposti né ai vincoli del comma 1 né a quelli del comma 3 in tema di utilizzabilità.

Questa interpretazione è coerente con le dinamiche di liberalizzazione dei controlli. Infatti la riconduzione nell'alveo dei controlli preterintenzionali non determina più l'inutilizzabilità dei dati ai fini disciplinari garantendo comunque al lavoratore il rispetto della procedura autorizzativa dei vincoli inerenti il rapporto di lavoro. Tuttavia in merito all'installazione e all'impiego resta il

dubbio se possa essere installato lo strumento di controllo anche senza accordo o autorizzazione.

Il 2° comma dell'articolo 4 S.L pone rimedio al problema che era aperto, in riferimento agli strumenti di lavoro, relativamente alla questione se dovesse essere stipulato l'accordo o richiesta l'autorizzazione per il loro utilizzo da parte dei lavoratori. Infatti ora non è necessario né l'accordo né l'autorizzazione, per fornire al lavoratore gli strumenti di lavoro, ma è "solo" richiesto, il rispetto del codice della privacy.

In merito al secondo comma si apre il problema riguardo all'estendibilità del concetto di strumento di lavoro. Infatti il rischio è quello di far rientrare anche strumenti che, migliorando l'organizzazione e quindi l'efficienza della prestazione, di fatto non sono utili allo svolgimento della mansione. Questo cambiamento non deve essere visto tuttavia come un venire meno di tutele nei confronti del lavoratore. In realtà la tutela diventa più individuale che collettiva, si riduce lo spazio di azione del sindacato ma il lavoratore si vedrà più tutelato in merito alle informazioni personali e ai dati sensibili. La verifica della legittimità dei controlli potrà essere solo successiva e non preventiva. Saranno i giudici di merito a vagliare a posteriori l'adeguatezza delle policy e il rispetto della normativa sulla privacy. Questo porterà senza dubbio, all'interno delle aule, nuove tematiche finora poco affrontate.[76]

Gli strumenti di lavoro, a parere di chi scrive, saranno l'argomento più problematico. Questo lo si riscontra anche alla luce del chiarimento fornito dal Ministero del Lavoro (V. Paragrafo 2.2). Infatti se nel futuro gli strumenti tecnologici fossero, come è prevedibile, sempre più ricchi e sempre più in grado di fornire informazioni aggiuntive da usare ai fini del controllo a distanza del

[76] A. Bottini, "Più tutela individuale, si riduce lo spazio del nullaosta preventivo", *Il sole 24 ore*, 24 agosto 2016, p.29

lavoratore, potranno essere utilizzate? Inoltre anche i criteri per stabilire se uno strumento sia o meno di lavoro restano indefiniti. Questo Comporta non pochi problemi per le aziende. Infatti l'installazione o l'utilizzo senza accordo sindacale o autorizzazione è ancora sanzionabile penalmente. Invece per gli strumenti di rilevazione degli accessi e delle presenze l'accordo sindacale non è previsto tuttavia l'assenza dell'informativa ai sensi del Codice della Privacy, comporta l'inutilizzabilità delle informazioni raccolte.[77]

In merito alla nota del ministero anche l'ufficio giuridico e vertenze, rilasciando un commento all'art. 4 dello Statuto dei lavoratori, ha ritenuto che l'interpretazione fornita dal Ministero di fatto non trovi spazio per come posta la norma in quanto se lo strumento è utilizzato per effettuare la prestazione allora, anche se installato successivamente, è lecito effettuare il controllo.[78]

Per quanto riguarda la "convivenza" con l'articolo 8 della L. n. 148/2011 sembra che la norma come abbiamo già visto nel capitolo 2 possa essere derogata in *melius* o in *pejus* da parte della contrattazione collettiva facendo anche ipotizzare dei limiti più stringenti rispetto a quanto previsto dalla norma. Tuttavia si ritiene pacifico che non possa essere prevista nel CCNL l'inutilizzabilità dei dati ai fini disciplinari.[79]

Il nuovo articolo offre, oltre a una nuove aperture, anche maggiori certezze alle aziende, e al lavoratore andando a inserire l'obbligo dell'informativa e il rispetto del Codice della Privacy. Questo è un elemento fondamentale che porta la norma a un livello di maturità nuovo facendo comunicare le due discipline in maniera tale da consentire una maggiore equilibratura degli interessi in gioco. A questo si potrebbe obiettare che lo scambio è ineguale, perché quelle garanzie già c'erano.

[77] A. Bottini, "A braccetto privacy e diritto del lavoro", *Il sole 24 ore*, 24 agosto 2016, p.29
[78] Ufficio giuridico e vertenze CGIL, "primo commento sulla revisione art. 4 statuto sui controlli a distanza", p.3
[79] M. Tiraboschi, *Le Nuove regole del lavoro dopo il Jobs Act*, Giuffrè Editore, 2015, p.122.

È vero che già c’erano, ma soltanto sulla carta. Infatti come abbiamo visto anche nel filone giurisprudenziale dei controlli difensivi la privacy non veniva quasi mai considerata.

Sarà importante infatti vedere quali saranno le disposizioni fornite dal Garante che, presumibilmente, andranno a porre regole chiare sulle modalità di utilizzo e di raccolta delle informazioni. È evidente che al termine di quest’analisi le domande restano e si dovrà vedere quali saranno le interpretazioni che saranno accolte dalla giurisprudenza. In ogni caso è consigliabile e prudente che le parti interessate si attivino momentaneamente per chiarire di comune accordo le forme in cui i controlli a distanza potranno essere effettuati ed evitare così le incertezze derivanti dalla mancanza di precisi orientamenti giurisprudenziali.

BIBLIOGRAFIA

Addonizio, V., Altimari, M., Biagioni, T., Borali, M., Chellini, S., Chiusolo, S., . . . Fezzi, M. (2015). Guida al Jobs Act. *I quaderni di wikilabour*.

Alberici, D. (2016, Agosto 2). Video riprese anti-fannulloni. *Italia Oggi*, p. 27.

Alvino, I. (2016). I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello statotuto dei lavoratori e quelle del Codice della Privacy. *Labour & Law Issues, 2*(1).

Bottini, A. (2016, Agosto 24). A braccetto privacy e diritto del lavoro. *Il Sole 24 Ore*, p. 29.

Bottini, A. (2016, Agosto 24). Dipendenti informati su telecamere e tablet. *Il sole 24 ore*, p. 28.

Bottini, A. (2016, Agosto 24). Necessari regolamenti aziendali dettagliati, chiari e completi. *Il Sole 24 Ore*, p. 28.

Bottini, A. (2016, Agosto 24). Valutazioni differenti sulla "natura" del Gps. *Il Sole 24 Ore*, p. 28.

Caiazza, L., & Caiazza, R. (2016, Giugno 8). La videosorveglianza richiede l'accordo. *Il sole 24 ore*.

Cairo, L. (2016). Il controllo a distanza dei lavoratori: precedenti nella giurisprudenza di ieri decisi con le norme di oggi. *Labour & Law Issues, 2*(2).

Carinci, M. T. (2016). Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art.23 D.Lgs. 151/2015): Spunti per un dibattito. *Labour & Law Issues, 2*(1).

Castellaneta, M. (2016, Gennaio 13). Controllabile la mail aziendale. *Quotidiano del lavoro*.

CGIL. (2015, Luglio 8). Primo commento sulla revisione art. 4 statuto su controlli a distanza. Roma.

Cirioli, D. (2016, Giugno 18). Telecamere Ko senza l'accordo presciozione obbligatoria se l'installazione è illecita. *Italia Oggi*, p. 38.

Corso, M., Crespi, R., & Scacco, A. C. (2016). *Smart Working.* Milano: Il sole 24 ore.

Cosattini, L. (2015). Le modifiche all'art. 4, Stat. lav. sui controlli a distanza, tanto rumore per nulla? *Il lavoro nella giurisprudenza*.

Ghini, P., & Colombi, I. (2016). Controllo degli accessi in azienda. *Riviste 24*.

Gigliotti, A. (2016, Giugno 22). Videosorveglianza: le modalità operative del controllo. *Fiscal Focus*.

Iaselli, M. (2016). *La privacy per lo studio professionale.* Milano.

L. D'Andrea, E. M. (2016). controlli a distanza: La disciplina prima e dopo la riforma. *Diritto e Pratica del LAvoro*.

Massi, E. (2016). La nuova videosorveglianza. *Guida alle paghe*.

Messina, A. C. (2016, Febbraio 8). Controlli a distanza, un rebus per imprese e lavoratori. *Italia Oggi*.

Messina, A. C. (2016, Febbraio 8). Il codice della privacy non basta. *Italia Oggi*.

Punta, R. D. (2015). *Diritto del Lavoro.* Milano: Giuffrè .

Ricchiuto, P., & Messina, A. C. (2016, Giugno 20). Controlli, disciplinare da rifare. *Italia Oggi*.

Schiavione, R. (2015). *Controllo dei Lavoratori.* Milano: Gruppo 24ore.

Tiraboschi, M. (2015). *Le nuove regole del lavoro dopo il Jobs Act.* Milano: Giuffrè.

Ziccardi, G. (2016). Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico - giuridiche. *Labour & Law Issues, 2*(1).