

Dipartimento di Giurisprudenza

Cattedra di Diritto del Lavoro

Controllo a distanza sull'attività dei lavoratori:  
l'evoluzione della disciplina  
tra Jobs Act e tutela della privacy

Chiar.mo Prof. Roberto Pessi

---

RELATORE

Chiar.mo Prof. Raffaele Fabozzi

---

CORRELATORE

Giulia Li Greci – Matr. 137373

---

CANDIDATO

Anno Accademico 2019/2020

## INDICE

<b>INTRODUZIONE.....</b>	<b>p. 5</b>
<b>CAPITOLO I : PROFILO STORICO E SISTEMATICO DEI CONTROLLI SUI LAVORATORI</b>	
<b>1. Il controllo nella sua evoluzione storico-normativa.....</b>	<b>p. 8</b>
1.1 Il controllo: dalla visione di Jeremy Bentham a quella di George Orwell.....	p. 8
1.2 I cambiamenti organizzativi apportati dalla II rivoluzione industriale.....	p. 12
1.3 Il contratto di lavoro subordinato nel codice civile del 1865 e nel pensiero di Lodovico Barassi.....	p. 16
1.4 Il codice del 1942.....	p. 19
1.5 La Costituzione e la normativa sovranazionale.....	p. 22
<b>2. Il datore di lavoro e i suoi poteri.....</b>	<b>p. 23</b>
2.1 Il potere di controllo.....	p. 24
2.2 Il potere direttivo.....	p. 28
2.3 Il potere disciplinare.....	p. 29
<b>3. Il controllo a distanza nella versione originaria dell'art. 4 dello Statuto dei lavoratori.....</b>	<b>p. 31</b>
3.1 I controlli intenzionali.....	p. 32
3.2 I controlli preterintenzionali.....	p. 36
3.3 I controlli difensivi.....	p. 43
<b>4. Il diritto alla riservatezza: profili introduttivi.....</b>	<b>p. 62</b>
4.1 Le origini del concetto di privacy negli Stati Uniti D'America.....	p. 62
4.2 Il diritto di privacy: quadro nazionale e comunitario.....	p. 64
<b>CAPITOLO II: IL CONTROLLO A DISTANZA ALLA LUCE DEL JOBS ACT</b>	
<b>1. Esigenze di riforma: il contesto che fa da innesco all'art. 23 del d.lgs. n. 151/2015.....</b>	<b>p. 71</b>

<b>2.</b>	<b>L'articolo 4 dello Statuto dei lavoratori come effetto del Jobs Act.....</b>	<b>p. 73</b>
2.1	La rimodulazione dei controlli: il nuovo comma 1.....	p. 74
2.2	Le novità procedurali.....	p. 79
2.3	Il comma 2: le nuove categorie di strumenti.....	p. 84
<b>3.</b>	<b>L'utilizzabilità dei dati raccolti e la tutela della riservatezza del lavoratore.....</b>	<b>p. 92</b>
3.1	La regola generale dell'utilizzabilità e l'informazione al lavoratore.....	p. 92
3.2	La trasparenza del trattamento delle informazioni registrate.....	p. 97
3.3	La tutela della privacy: la seconda condizione di utilizzabilità dei dati raccolti.....	p. 100
3.3.1	Il Regolamento (UE) n. 679/2016 e il d.lgs. n. 101/2018: i due poli della tutela della riservatezza in materia di controllo a distanza.....	p. 101
3.3.2	Privacy by default e privacy by design.....	p. 109
3.3.3	La valutazione d'impatto sui dati personali.....	p. 114
<b>4.</b>	<b>Il regime sanzionatorio.....</b>	<b>p. 117</b>
<b>5.</b>	<b>I mezzi di controllo e le nuove tecnologie.....</b>	<b>p. 120</b>
5.1	Videosorveglianza.....	p. 120
5.2	Social network.....	p. 130
5.3	BYOD e LOG.....	p. 134
5.4	Internet e posta elettronica.....	p. 137
5.5	Geo-localizzazione.....	p. 141

### **CAPITOLO III: DALLA NORMA AL CASO CONCRETO**

<b>1.</b>	<b>Il braccialetto elettronico: la nuova tecnologia made in Amazon.....</b>	<b>p. 146</b>
1.1	Il braccialetto elettronico: strumento dal quale deriva anche la possibilità di controllo a distanza o strumento di lavoro?.....	p. 149
1.2	Il braccialetto elettronico e la privacy.....	p. 150
	<i>Segue. L'avvento dei microchip: dall'americana Three Square Market</i>	

	all'italiana Fincantieri.....	p. 152
<b>2.</b>	<b>La videosorveglianza alla luce della giurisprudenza CEDU.....</b>	<b>p. 155</b>
2.1	<i>Ante</i> López Ribalda e altri v. Spagna: Bărbulescu v. Romania e Antović e Mirković v. Montenegro.....	p. 156
2.2	López Ribalda e altri v. Spagna: la versione della Camera semplice....	p. 162
	<i>Segue.</i> Una lettura congiunta delle sentenze della Corte EDU.....	p. 168
2.3	López Ribalda e altri v. Spagna: il cambio di rotta della Grande Camera.....	p. 172
	<b>CONCLUSIONI.....</b>	<b>p. 178</b>
	<b>BIBLIOGRAFIA.....</b>	<b>p. 181</b>

## INTRODUZIONE

Lo sviluppo delle nuove tecnologie ha rivoluzionato gli ambienti di lavoro, influenzando non solo le modalità di esecuzione della prestazione lavorativa, ma anche le potenzialità del controllo datoriale: tale situazione ha reso consequenzialmente di estrema attualità il tema dei limiti entro cui i controlli, anche se essenziali al datore per la gestione del rapporto, devono essere confinati a tutela dei diritti della persona del lavoratore, della sua dignità e riservatezza. Dopo la ricostruzione sia del concetto di controllo, sia dell'evoluzione della figura del lavoratore subordinato, che da soggetto completamente inserito nella compagine aziendale, tenuto all'obbedienza e fedeltà al suo datore di lavoro, coerentemente con l'ideologia paternalistica e autoritaria degli anni '40, è passato a essere riconosciuto come persona alla quale si deve il rispetto della dignità e della libertà, giacché non più sottomessa al proprio datore di lavoro, si approfondirà la disciplina dell'art. 4 dello Statuto dei lavoratori, disposizione con cui per la prima volta nel nostro ordinamento sono stati disciplinati i controlli a distanza.

Il vaglio di cui la disposizione sarà oggetto investirà tanto la sua versione originaria, quanto il suo nuovo testo, frutto della riforma operata dal c.d. Jobs Act nel 2015, in particolare dall'art. 23 del d.lgs. n. 151/2015. Tale riforma deve interpretarsi come un'opera di aggiornamento, funzionale a rendere una normativa risalente nel tempo e obsoleta, attuale.

Si tenterà così di evidenziare il passaggio da una disposizione che sanciva esplicitamente il divieto assoluto dei controlli intenzionali, nonché la legittimità di quelli preterintenzionali a certe condizioni, a una disposizione che, in primis, ha mantenuto il ricordato divieto assoluto di controllo a distanza dell'attività lavorativa solo a livello implicito e, in secondo luogo, quanto ai controlli indiretti, è andata ad aggiungere una nuova esigenza a quelle che, originariamente previste, già li legittimavano. L'ingresso della "tutela del patrimonio aziendale", voluto dal Jobs Act, non è di certo passato inosservato, avendo riaperto la discussione sulla categoria, di matrice giurisprudenziale, dei cd. controlli difensivi, frutto di una già intensa attività interpretativa caratterizzata, storicamente, da un percorso tutt'altro che lineare e segnato da due opposti orientamenti che si tenterà di sviluppare. La giurisprudenza, alla luce di questa evoluzione, è stata costretta a modellare l'articolo 4 in accordo con le nuove esigenze creatisi, espletando un'importante attività per individuare i limiti alle varie tipologie di controllo modellate indirettamente dalle nuove tecnologie. Al lavoro giurisprudenziale si è poi affiancata l'evoluzione della tutela della privacy dei lavoratori, che è stata oggetto di un'apposita normativa, sviluppatasi su due piani, nazionale e comunitario, ovvero sia il d.lgs. n. 196/2003 e il fascio di raccomandazioni e

regolamenti europei che hanno portato gli Stati membri ad adottare una serie di regole utili a creare una tutela minima uniforme all'interno del territorio europeo. Infatti, come si esaminerà, insieme all'esclusione dei cd. strumenti di lavoro e di quelli volti alla registrazione degli accessi e delle presenze dall'ambito di operatività dei controlli a distanza dell'attività lavorativa per le finalità e le procedure previste dalla norma medesima, un'altra grande novità introdotta dal nuovo testo dell'art. 4 è proprio la previsione di una specifica disposizione sulla tutela della riservatezza e della dignità del lavoratore, che rivela la centralità conquistata nel corso degli anni dalla privacy. I controlli tecnologici hanno introdotto il delicato tema della protezione dei dati personali giacché le imprese automatizzate e a elevato sviluppo informatico sono in grado di immagazzinare, archiviare e utilizzare consistenti flussi di dati, fornendo all'impresa ingenti informazioni circa i propri dipendenti. Si tenterà di evidenziare come, con l'ultimo comma dell'art. 4 St. lav., il Legislatore abbia aggiornato la disciplina del potere di controllo, regolamentando tutte le fasi della relativa attività di controllo in vista del soddisfacimento del bisogno di protezione della dignità e della riservatezza del lavoratore; è ora disciplinata anche quella fase che si colloca a valle del controllo, a questo punto superato, essendo le informazioni entrate nella disponibilità del datore di lavoro, il quale potrà sfruttarle a distanza di tempo o luogo dal momento della loro acquisizione.

È in questo quadro che si colloca il rispetto di quanto disposto dal Codice privacy, per come modificato dal d.lgs. n. 101/2018 volto ad adeguare il Codice privacy stesso al nuovo Regolamento europeo generale sulla protezione dei dati (GDPR) n. 679 del 2016, il quale al suo quinto articolo, sancisce i principi per il trattamento dei dati personali, al cui rispetto è subordinato l'esercizio del potere di controllo del datore di lavoro. La legge delega n. 183/2014, base dell'intera riforma del Jobs Act, non faceva alcun cenno all'integrazione della specifica materia in commento tra livello regolativo nazionale e sovranazionale e, difatti, i decreti legislativi del 2015 non sono maturati in un contesto di stretta armonizzazione. Nonostante ciò, si vedrà che l'interpretazione del doppio binario normativo che si desume dall'art. 4, comma 3, St. lav., ad oggi, rappresenta un settore foriero di questioni interpretative, anche sul piano della c.d. privacy multilivello.

Con il presente lavoro si tenterà quindi di mettere l'accento anche sulla necessità di bilanciare il rispetto dei diritti del datore di lavoro, espressione degli scopi economici della realtà imprenditoriale, con quelli del lavoratore nell'esecuzione della prestazione lavorativa, senza tralasciare l'analisi dell'evoluzione europea del quadro normativo in materia di tutela della riservatezza.

Nella parte conclusiva dell'elaborato ci si appresterà infine a vagliare più da vicino le apparecchiature tecnologiche oggi presenti nel mondo del lavoro: d'altronde lo scenario tecnologico

che ha visto nascere la norma esaminata era dominato, quanto ad apparecchiature, da telecamere aziendali a circuito chiuso associate alle catene di montaggio; il Legislatore non poteva neanche lontanamente immaginare che sarebbe sorta la necessità di adeguare l'art. 4 St. lav. non solo a un contesto, come si approfondirà, capitanato da una videosorveglianza nettamente più avanzata, oggetto di un percorso evolutivo della giurisprudenza europea decisamente non uniforme, da internet, posta elettronica, e sistemi di geo-localizzazione, ma anche un contesto che rischia di conoscere braccialetti elettronici e microchip sottocutanei come quotidianità e non più fantascienza.

## CAPITOLO I

### PROFILO STORICO E SISTEMATICO DEI CONTROLLI SUI LAVORATORI

#### 1. Il controllo nella sua evoluzione storico – normativa

Il diritto del lavoro è lo strumento con cui il legislatore, garantendo un intervento governativo, risponde alle sollecitazioni provenienti dal mondo dell'economia e della società. La sua specialità risiede nel diretto e totale coinvolgimento delle persone, le quali nell'attività lavorativa trovano non soltanto un mezzo di sostentamento, ma anche un mezzo per la piena realizzazione sociale. Se è innegabile che il sistema del diritto del lavoro debba tener conto delle ragioni di entrambi i soggetti coinvolti nel rapporto in quanto, il contratto, sia esso collettivo o individuale, *“riguarda l'avere per l'imprenditore ma, allo stesso tempo, per il lavoratore riguarda e garantisce l'essere, il bene che è condizione dell'avere e di ogni altro bene”*<sup>1</sup>, è allo stesso tempo cristallino che il diritto del lavoro sia nato e tradizionalmente si sia sviluppato in direzione protettiva del lavoratore subordinato, occupandosi *“non tanto del lavoro in sé, quanto soprattutto di chi lavora (...) un diritto più della persona che dell'attività”*<sup>2</sup>.

#### 1.1 Il controllo: dalla visione di Jeremy Bentham a quella di George Orwell

Uno dei conflitti che permea il mondo lavorativo è quello tra interesse del datore di lavoro al controllo dei propri dipendenti e interesse del lavoratore alla riservatezza.

Partendo dall'analisi del concetto di controllo e retrocedendo alla fine del secolo XVIII, precisamente al 1791, riscontriamo come la nozione affondi le sue radici nella figura del *Panopticon*, figlia del filosofo e giurista inglese Jeremy Bentham; d'altro canto, volgendo per un istante lo sguardo verso la società odierna, è innegabile come gli occhi del sorvegliante del Panopticon siano stati sostituiti dagli occhi delle telecamere e, in seguito, dal ben più invasivo occhio del web.

Nel libro I del Capitale, Karl Marx, laddove avvertiva che sarebbe passato a trattare la sfera della produzione, ovvero *“la concia”* dei lavoratori, dichiarava che fino a quel punto aveva analizzato la sfera della circolazione, ove *“regna solo libertà uguaglianza, proprietà e Bentham”*<sup>3</sup>. Progettato inizialmente come struttura carceraria, il Panopticon di Bentham ha cominciato ben presto a essere considerato come una vera e propria forma rivoluzionaria ideale per concepire ogni generica costruzione. Nel suo progetto, il filosofo inglese ipotizzava che il sistema di organizzazione e di sorveglianza, escogitato per il suo carcere modello, potesse essere esteso anche

---

<sup>1</sup> SANTORO PASSARELLI F., *Spirito del diritto del lavoro*, in Saggi di diritto civile, Napoli, 1959.

<sup>2</sup> MISCIONE M., *Dialoghi di diritto del lavoro*, Milano, 2011.

<sup>3</sup> MARX K., *Il Capitale*, Libro I, Torino, 2011.

ad altre strutture, ove molte persone si trovassero riunite e sottoposte a una comune disciplina, come, a titolo esemplificativo, gli istituti dove poter combattere l'indigenza con il lavoro<sup>4</sup>. *“Poco importa se lo scopo dell'edificio è diverso o anche opposto: sia che si tratti di punire i criminali incalliti, sorvegliare i pazzi, riformare i viziosi, isolare i sospetti, impiegare gli oziosi, mantenere gli indigenti, guarire i malati, istruire quelli che vogliono entrare nei vari settori dell'industria, o fornire l'istruzione alle future generazioni: in una parola sia che si tratti di prigionieri a vita (...) o case di lavoro o fabbriche o manicomi o ospedali o scuole”*<sup>5</sup>. Composto da una torre di sorveglianza centrale, con attorno un anello periferico in cui sono sistemati coloro che devono essere controllati, il Panopticon aveva come scopo quello di permettere a un solo sorvegliante di controllare una moltitudine di persone senza essere visto, osservando (*opticon*) ogni soggetto (*pan*), ridotto a oggetto del controllo da parte del potere. Gli individui da “soggetti di una comunicazione” sono trasformati in prigionieri, ovverosia “oggetti d'informazione”. A ben guardare, si tratta di un'impostazione che evoca quella relazione di carattere generale soggetto – oggetto, che sarà poi trasposta dalla sorveglianza elettronica nel secolo XX, riducendo le persone a data – immagini: gli oggetti dello “sguardo” digitale non possono trascinare la loro vista nel database, più di quanto i detenuti del Panopticon potessero guardare nella rotonda centrale<sup>6</sup>.

In tale struttura si cercava una tecnica che assicurasse il funzionamento automatico del sistema, in modo da garantire la certezza organizzativa al prezzo dell'incertezza dei detenuti. L'impossibilità di verificare l'esercizio attuale del potere di controllo, ossia l'impossibilità fisica, dovuta alla particolare configurazione del Panopticon, di osservare l'interno della torre di controllo è dallo stesso Bentham sottolineata come una delle intrinseche qualità del progetto in un'ottica di riduzione dei costi, efficienza, semplicità e automazione, il cui obiettivo è far crescere e moltiplicare. Di qui l'effetto principale del Panopticon: indurre nel detenuto uno stato cosciente di visibilità che assicura il funzionamento automatico del potere. Far sì che la sorveglianza sia permanente nei suoi effetti, anche se discontinua nella sua azione<sup>7</sup>.

Prigioni, fabbriche, uffici, lo stato con i servizi segreti e le polizie segrete e oggi la rete con social e Big Data richiamano quel modello: un meccanismo di potere che produce un dispositivo di sorveglianza e di controllo, ma anche, in chi deve essere osservato, una sorta di auto-sorveglianza e di auto-controllo, come censura su se stessi per introiezione dei comportamenti prescritti, a fronte del dubbio di essere o meno osservati dalla torre<sup>8</sup>.

---

<sup>4</sup> DE BONI C. (a cura di), *Lo stato sociale nel pensiero politico contemporaneo: L'Ottocento*, Firenze, 2007.

<sup>5</sup> BENTHAM J., *Panopticon, ovvero la casa d'ispezione*, FOUCAULT M. - PERROT M. (a cura di), Venezia, 1983.

<sup>6</sup> LYON D., *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Milano, 1997.

<sup>7</sup> GIUSTO N., *Foucault, Panopticon e ordine disciplinare*, su [www.culturedigitali.org](http://www.culturedigitali.org).

<sup>8</sup> PECCHIOLI R., *La società della sorveglianza. Totalitarismo del terzo millennio*, su [www.ariannaeditrice.it](http://www.ariannaeditrice.it).

Veniva teorizzato un modo quasi perfetto per costruire uomini docili e produttivi. Produttivi di lavoro nella fabbrica-fordista, di dati nella fabbrica-rete<sup>9</sup>.

Con Bentham si diffuse la convinzione che l'accrescimento del potere della macchina panoptica non sarebbe potuto degenerare in tirannia, anzi si pensava che avrebbe garantito sicurezza e libertà, in quanto il meccanismo disciplinare sarebbe stato controllato democraticamente, perché accessibile in ogni momento al grande comitato del tribunale del mondo. In realtà, quello che Bentham aveva sottovalutato era che se il controllo sugli individui è capillare e pervasivo, il controllo sul controllo e su chi o cosa controlla è quasi del tutto assente. Questa è la logica del potere.

Se nella realizzazione pratica il progetto di Bentham non ha mai concretamente visto la luce, sul piano filosofico-metaforico ha avuto un grande successo.

La casa d'ispezione del giurista inglese è diventata metafora di un potere invisibile, senza volto e pervasivo utilizzata da grandi figure, come il filosofo Michel Foucault nella sua opera "Sorvegliare e Punire" e lo scrittore George Orwell, che ne ha fatto il modello di partenza per il suo romanzo "1984".

Michel Foucault ne fa uno degli elementi cardine della sua analisi sul sorvegliare e punire, ossia sul vigilare la classe lavoratrice per poterla punire ogni qual volta assuma comportamenti antitetici al capitale<sup>10</sup>, e sulla nascita della prigione moderna, delle discipline, quindi del capitalismo<sup>11</sup>. Non importa che una telecamera sia diretta verso alcuni luoghi invece di altri, conta che il padrone possa installare impianti per costruire un clima di paura, anche senza assenso sindacale e con quella pressione psicologica sui singoli, che assume la valenza di un ricatto vero e proprio. Gli operai rassegnati e intimoriti saranno disposti ad accogliere aumenti dei ritmi; sapranno di essere vulnerabili e facili da colpire; si adegueranno velocemente ai dettami aziendali. Significativo in tale direzione è come Foucault definisce il Panopticon, una architettura del potere o meglio, con le sue parole, *"una microfisica di sapere e poteri di controllo e di induzione all'autocontrollo"*. Il Panopticon, per Foucault, permette di perfezionare e di potenziare l'esercizio del potere e di farlo in molti modi: riducendo il numero di coloro che lo esercitano, ma allo stesso tempo moltiplicando il numero di soggetti/oggetti sui quali si esercita; intervenendo incessantemente perché la sua forza è di esercitarsi spontaneamente e senza rumore; divenendo un meccanismo i cui effetti si concatenano gli uni agli altri, creando una società penetrata da meccanismi disciplinari e arrivando

---

<sup>9</sup> DEMICHELIS L., *Sorvegliati e contenti: così i social hanno realizzato la forma di controllo perfetta*, su [www.agendadigitale.eu/cultura-digitale/](http://www.agendadigitale.eu/cultura-digitale/).

<sup>10</sup> GIUSTI F., *Videosorveglianza: il Panopticon del XXI secolo*, su [www.cittafutura.it/economia-e-lavoro/](http://www.cittafutura.it/economia-e-lavoro/).

<sup>11</sup> GIANNETTI L., *Una prigione di telecamere, un Panopticon moderno?*, su [www.ilsuperuovo.it](http://www.ilsuperuovo.it).

alla società della sorveglianza di oggi. Una società in cui alcuni soggetti, oggi soprattutto le imprese, dispongono di un archivio dettagliatissimo di dati personali, da quelli anagrafici ai gusti, alle disposizioni a malattie, permettendo un controllo anche più invasivo di quello immaginato da Bentham e poi da Orwell in “1984”. A detta di Foucault *“il Panopticon è una macchina per dissociare la coppia vedere-essere visti: nell’anello periferico si è totalmente visti, senza mai vedere (il sorvegliante); nella torre centrale si vede tutto, senza mai essere visti”*<sup>12</sup>.

Un sorvegliante che controlla tutte le altre persone, spingerà progressivamente queste ultime a comportarsi nel modo desiderato dal sorvegliante, anche in sua assenza non sapendo più se sono, in ogni momento, sorvegliati o meno. D’altro canto *“quanto più un potere è in vista, tanta meno autorità possiede, mentre meno è conosciuto e riconoscibile tanto più potente diventa”*<sup>13</sup>.

Tenendo presente ciò, è chiaro come emerga in superficie non solo il problema della privacy, del riconoscimento del diritto alla riservatezza dei lavoratori, ma anche il bisogno di dare ai lavoratori stessi la possibilità di difendersi dall’aumento dei ritmi e da uno sfruttamento intensivo, che ha aumentato lo stress correlato al lavoro, gli infortuni e i malesseri legati a una condizione subalterna, che va scivolando nella schiavitù. D’altronde, il risultato dell’assenza di privacy e la connessa integrale trasparenza di ciascuno, rispetto a un potere non visibile, non possono che postulare inevitabilmente un uomo di vetro<sup>14</sup>.

Come anticipato, l’altra opera che ha risentito dell’idea del Panopticon è “1984”. Nella società che Orwell descrive, ciascun individuo è tenuto costantemente sotto controllo dalle autorità e lo slogan *“Il Grande Fratello vi guarda”* ricorda continuamente agli abitanti la sua superiorità assoluta nella piramide gerarchica.

Negli anni settanta e ottanta del secolo XX l’attenzione dei datori di lavoro era rivolta, soprattutto, all’utilizzo degli apparecchi telefonici aziendali e a ciò che si svolgeva all’interno degli ambienti dell’azienda: per averne contezza non era infrequente allestire pareti di vetro trasparenti, finestre o telecamere. Il sistema di controllo era “classico”, proprio in puro stile orwelliano: un centro che, grazie a telecamere spesso poste in luoghi segreti, controlla in tempo reale, consentendo una sorveglianza occulta. Accanto alla tecnologia, ben di più poteva la tecnica tradizionale, ossia l’uso di schedari compilati grazie a informazioni provenienti, in quegli anni, soprattutto dalle fonti presso le parrocchie e le questure. La vita lavorativa, comprese posizioni sindacali e opinioni politiche del

---

<sup>12</sup> FOUCAULT M., *Sorvegliare e punire*, Torino, 2008.

<sup>13</sup> ARENDT H., *Le origini del totalitarismo*, Torino, 2004.

<sup>14</sup> L’uomo di vetro nasce come metafora nazista. Essa legittima la pretesa dello Stato di chiedere e ottenere qualsiasi informazione, implicando la classificazione come “sospetto”, “cattivo cittadino”, infine “nemico dello Stato” di chiunque intenda mantenere spazi d’intimità, di esercizio libero di diritti, sul convincimento che la sorveglianza continua e generalizzata e la cancellazione di ogni ragionevole brandello di privacy possano costituire un problema solo per chi ha qualcosa da nascondere.

sorvegliato, era controllata tramite le prime tecnologie; la vita privata, tranne casi eccezionali, si ispezionava raccogliendo informazioni e compilando dossier.

Come si passerà in rassegna, lo Statuto dei lavoratori cercò, tra l'altro, proprio di evitare questi fenomeni di controllo occulto visti, allora, come la modalità più invasiva e subdola esistente.

## **1.2 I cambiamenti organizzativi apportati dalla II rivoluzione industriale**

La rivoluzione industriale ha rappresentato un terreno fertile da cui partire per prendere in considerazione e sviluppare la tutela del lavoratore come uomo che lavora, non più come mero proprietario della propria forza lavoro<sup>15</sup>.

*“Insegna Mattia Persiani che le radici del Diritto del lavoro affondano nel terreno del conflitto industriale determinato dal modello di produzione capitalistica che contrappone, inevitabilmente, chi detiene i mezzi di produzione a chi vive della produzione”*<sup>16</sup>.

La maggiore espressione della rivoluzione industriale in termini di organizzazione è stata il sistema di fabbrica, la cui affermazione ha determinato il passaggio da un'organizzazione produttiva di stampo agricolo e artigianale a un'organizzazione strutturata sull'impresa capitalistica. Nel primo modello di organizzazione a dominare era la bottega artigiana, fulcro dell'economia pre-industriale: in essa, i collaboratori dell'artigiano prestavano la loro opera non in funzione di un corrispettivo, ma per apprendere un mestiere, producendo un risultato destinato a soddisfare le limitate esigenze della vita cittadina o di corte.

Il sistema di fabbrica ha rivoluzionato questa realtà. Innanzitutto si sono affermate nuove figure: da un lato i padroni, proprietari del capitale necessario agli investimenti in macchine e al pagamento dei salari degli addetti al loro funzionamento, e dall'altro gli operai, che vendevano la loro forza lavoro. In tale apparato, tutte le fasi del processo produttivo si sono accentrate in un unico luogo, alle dipendenze dell'imprenditore, allo scopo di giungere a una produzione di serie dei manufatti<sup>17</sup>. L'utilizzazione delle macchine per la produzione su vasta scala, oltre a consentire il sorpasso dell'opera manuale, ha portato sempre più a concentrare masse di lavoratori in fabbriche organizzate secondo criteri razionali con funzioni, orari, ritmi definiti in base alle esigenze della divisione del lavoro. Nasceva dunque da un lato, la figura del capitalista industriale, imprenditore proprietario della fabbrica interessato a ottenere un profitto, e dall'altra quella della classe operaia, che in cambio di una certa prestazione o del tempo messo a disposizione nel lavoro in fabbrica, otteneva un salario.

---

<sup>15</sup> PROSPERETTI G., *Dalla tutela del rapporto di lavoro*, in Riv. Infortuni, 1994, p. 4.

<sup>16</sup> PESSI R., *Impresa e diritto del lavoro*, in Gnosis – Rivista italiana di intelligence n.4/2008.

<sup>17</sup> MAZZOTTA O., *Diritto del lavoro*, Milano, 2013.

E un esempio di capitalismo dal volto umano arrivava dall'Inghilterra. Nel 1851 tra le colline dello Yorkshire occidentale, non lontano dalla località di Bradford, venne realizzato il villaggio modello di Saltaire dall'industriale Sir Titus Salt. Quest'ultimo prestò molta attenzione all'ordine interno del suo villaggio. Nella grande filanda, che dava lavoro a circa tremila operai, le macchine erano allineate in lunghe file ordinate, facilmente controllabili dai capireparto. Al di fuori della fabbrica, la gerarchia dell'ordine era riprodotta nell'architettura, non lasciando nulla al caso: la schiera di case operaie lungo la strada veniva interrotta ogni tanto da abitazioni leggermente più grandi, quelle dei capireparto e delle loro famiglie. In questo modo vi era una sorta di controllo anche all'esterno del luogo in cui gli operai eseguivano le loro mansioni.

Come anche sottolineato dall'autore J. Reynolds nel 1983, Saltaire, uno dei numerosi insediamenti industriali sviluppati da grandi datori di lavoro della metà secolo XIX, era un villaggio aziendale soggetto al controllo di un datore di lavoro<sup>18</sup>. Si può dunque notare il rapporto tra sorveglianza e controllo sociale nel contesto lavorativo capitalista: il locale, lo spazio fisico in cui si svolgeva la produzione, è controllato mediante una super visione organizzativa.

Il problema che dovevano affrontare molti datori di lavoro all'inizio dell'era industriale era come controllare grandi masse di persone sul lavoro, senza adoperare la forza fisica, tipica della schiavitù. La risposta risiedeva nei nuovi metodi di gestione industriale: il lavoratore stilava un contratto con il padrone per guadagnarsi di che vivere, e a sua volta, il datore di lavoro controllava strettamente le attività degli operai. Il controllo veniva dunque concepito come un metodo di disciplina. Imporre delle sanzioni e offrire incentivi economici assicuravano tale controllo<sup>19</sup>.

Non avendo Sir Titus Salt lasciato dichiarazioni scritte sui propri scopi per la creazione di Saltaire, numerosi accademici e scrittori hanno tentato di rintracciare le ragioni che hanno fatto da innesco per il progetto di pianificazione della città industriale, dal 2001 inserita tra i Patrimoni dell'umanità. Nella sua valutazione del 2004, David James<sup>20</sup> ha espresso l'idea che i motivi siano scaturiti dalla combinazione del desiderio di sana economia e da quello di avere un controllo efficace sulla forza lavoro. Vi erano ragioni economiche per trasferirsi da Bradford, fornendo così il villaggio industriale a Salt una forza lavoro amabile e selezionata con cura.

Se da un lato l'industrializzazione ha favorito un certo sviluppo economico, specie a favore della borghesia capitalista, dall'altro l'inserimento nella fabbrica del lavoratore, che dalla campagna emigrava verso la città, non è apparso esente da aspetti negativi: il proletariato urbano viveva in

---

<sup>18</sup> SMITH M. – COATES C., *Salts Mill: The Owners and Managers 1853 to 1986*, Gloucestershire, 2016.

<sup>19</sup> LYON D., *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Milano, 1997.

<sup>20</sup> JAMES D., "Salt, Sir Titus, first baronet (1803–1876)", *Oxford Dictionary of National Biography*, Oxford University Press, 2004.

condizioni di miseria e sfruttamento estremi, le ore di lavoro giornaliera oscillavano dalle 12 alle 14, con turni di notte e senza ferie, gli ambienti di lavoro erano nocivi, in quanto quasi del tutto privi di illuminazione e mal areati, l'abbondante manodopera era sottopagata, spiccando salari estremamente bassi, limitati al livello di mera sussistenza, e infine i lavoratori non potevano fare affidamento su un impiego stabile, poiché ogni fase sfavorevole del ciclo produttivo causava ondate di disoccupazione, senza che essi potessero contare su alcuna forma di protezione sociale.

Questo scenario non risparmiava nemmeno le cd. mezze forze, ossia donne e minori, soggette a un massiccio sfruttamento in cui non solo si ritrovavano, al pari degli uomini, a operare in contesti insalubri con orari massacranti, ma erano anche sottopagate fortemente rispetto ad essi<sup>21</sup>.

La fotografia di questa realtà è stata scattata in maniera calzante dal filosofo e politico tedesco Karl Korsh, il quale riteneva che varcando il portone della fabbrica, casa del suo padrone, l'operaio venisse assoggettato a una legge particolare, data l'imposizione di norme di comportamento vincolanti. Per Korsh, promotore della costruzione di una teoria di democrazia industriale come parte integrante di una democrazia politica, la riflessione sui problemi connessi alla democrazia nei luoghi di lavoro scaturiva dalla ricerca di una via percorribile per superare, mediante lo strumento del controllo, la separazione tra governanti e governati, che escludeva la fabbrica dalle regole della democrazia. Il filosofo tedesco parlava della necessità di un controllo dal basso, esercitabile sui luoghi di lavoro, sulle sue condizioni e sull'organizzazione, per arrivare a un controllo della gestione delle imprese. Parlava di un controllo sfruttabile come strumento per coniugare il processo di autoliberazione della classe operaia, e quindi di attribuzione di una forma diretta di determinazione delle condizioni di lavoro, con una democrazia della rappresentanza, in grado di esprimere gli interessi dell'intera collettività. Un controllo che non andava a eliminare, utopisticamente, la sussistenza di forme di divisione del lavoro e di una struttura gerarchica, ma ne sottolineava la mutevolezza, la loro riformabilità, e il fatto di non essere insindacabili. Un controllo dal basso conservativo di spazi effettivi di poteri nei luoghi di lavoro<sup>22</sup>.

L'industrializzazione, fra gli anni Settanta del secolo XIX e la prima guerra mondiale, ha fatto da scenario a profonde trasformazioni: l'instaurazione di uno strettissimo rapporto tra scienza, tecnologia e industria; l'evoluzione della tecnologia produttiva, delle comunicazioni e dei trasporti; il mutamento della produzione industriale, con l'intensificazione dei processi di concentrazione e ristrutturazione industriale.

---

<sup>21</sup> Il risultato dunque del fenomeno in sé della rivoluzione industriale, nonché delle sue conseguenze quali lo sviluppo tecnologico, il crescente fenomeno dell'inurbamento, lo sfruttamento dei lavoratori, la concentrazione delle attività produttive, l'incrementarsi della pericolosità del lavoro, con la conseguente ed esponenziale crescita di infortuni e malattie, spesso mortali è la cd. "questione sociale".

<sup>22</sup> TRENTIN B., *La città del lavoro: sinistra e crisi del fordismo*, Milano, 1997.

Le novità in questo campo sono arrivate dagli Stati Uniti D'America, dallo studio e dalle prime applicazioni della "organizzazione scientifica" del lavoro, teorizzata dall'ingegnere Frederick Winslow Taylor. Quest'ultimo è l'autore di "*The principles of scientific management*", pubblicato nel 1911, i cui principi conobbero un enorme successo. La cd. "*one best way*", il metodo migliore, più economico ed efficiente per ottenere un prodotto, si basa sulla scomposizione delle varie fasi del ciclo produttivo in sei operazioni, il più possibile elementari, scientificamente misurate e programmate, nonché sull'attribuzione a ogni operaio di tali semplici, meccaniche e ripetitive operazioni. Il taylorismo si è poi intersecato con le innovazioni organizzative introdotte nel 1913 nell'industria automobilistica da Henry Ford. A Ford, l'industriale che meglio di altri comprese le straordinarie potenzialità del metodo tayloristico, si deve la riorganizzazione dell'intero stabilimento attorno alla catena di montaggio, che unisce le diverse fasi del lavoro di assemblaggio dell'automobile portando i pezzi ai lavoratori, ciascuno dei quali, fermo al suo posto e sottoposto a un rigoroso controllo, si limita a eseguire una delle semplici operazioni che costituiscono il processo di produzione.

Tratta dal film "Tempi Moderni", è iconica la scena di un Charlie Chaplin alle prese con gli ingranaggi della catena di montaggio di una fabbrica, tentando invano di muoversi più veloce della catena di montaggio per guadagnarsi una pausa.

Nel suo attacco alla meccanizzazione della vita dei lavoratori, Chaplin metteva alla berlina la segmentazione del lavoro nelle sue varie componenti, favorendo un'analisi dei tempi e dei movimenti, con dettagliate istruzioni per ogni operaio: appunto si tratta del sistema noto come *scientific management*, gestione o direzione scientifica del lavoro<sup>23</sup>. Il controllo meccanizzato degli operai che producono automobili, piuttosto che mobili con parti standardizzate, fotografava il sistema del fordismo.

Nel 1914, Ford aveva raddoppiato la paga dei suoi dipendenti, ma l'aumento era subordinato ad alcune condizioni: una permanenza in fabbrica di almeno sei mesi, la conoscenza della lingua inglese e il riconoscimento di un buon punteggio da parte degli ispettori della Sezione sociologica dell'azienda, incaricati di monitorare non le capacità di lavoro, ma la loro vita privata. La Sezione sociologica era stata creata con lo scopo di valutare i propri dipendenti anche al di fuori del lavoro di fabbrica, ovverosia nella loro vita familiare, verificando, tra l'altro, se si fossero recati a messa la domenica ed entrando persino in camera da letto.

---

<sup>23</sup> In esso il lavoro intellettuale è concentrato nel "settore progettazione", ma le qualità umane si possono esprimere anche sulle macchine, e allora il processo di subordinazione del lavoro può essere ulteriormente semplificato: il culmine è la catena di montaggio di Henry Ford.

Ieri la Sezione sociologica, oggi da remoto, come vedremo, il controllo delle mail, piuttosto che delle telefonate, non sono altro che modi per creare una forma panottica o post-panottica di organizzazione e controllo<sup>24</sup>.

### **1.3 Il contratto di lavoro subordinato nel codice civile del 1865 e nel pensiero di Lodovico Barassi**

Avendo, il rapporto di lavoro, ricevuto una vera e propria regolamentazione giuridica a cavallo tra i secoli XIX e XX, non sempre i lavoratori subordinati sono stati destinatari di tutela e diritti. E costituendo la parte debole del contratto di lavoro, specie in passato subivano considerevolmente la supremazia del datore di lavoro.

Al fine di esaminare i poteri di cui è titolare il datore di lavoro, può essere utile un generale inquadramento del rapporto di lavoro subordinato, che permette di individuare la tipologia contrattuale e relazionale in cui tali poteri possono essere esercitati e che è stato oggetto di una profonda evoluzione, così come la tutela dei lavoratori.

Pur non esistendo ancora il diritto del lavoro, il contratto di lavoro era già noto nella legislazione della fine del secolo XIX e nella prassi; era invece sconosciuto al codice civile del 1865 che, lungi dal definire o distinguere il lavoro subordinato e autonomo, conteneva solo tre disposizioni richiamabili dal giurista per inquadrare le discipline di varia fonte<sup>25</sup> regolatrici dei rapporti tra industriali e operai salariati. In particolare inquadrava l'attività lavorativa nello schema della locazione all'art. 1570, il quale definiva la locazione di opere come "*un contratto, per cui una delle parti si obbliga a fare per l'altra una cosa mediante la pattuita mercede*".

Sin dai tempi più remoti, se si esclude il regime della schiavitù, strumento principale nell'epoca arcaica per l'utilizzazione del lavoro umano al servizio altrui, il lavoro libero è sempre stato inquadrato nell'ambito dell'istituto della locazione.

Nel diritto romano, la *locatio – conductio* richiamava molte più fattispecie rispetto all'attuale contratto di locazione dell'ordinamento italiano, tanto che a seconda che l'oggetto del contratto fosse la cosa, l'opera, o le energie lavorative, includeva rispettivamente: *locatio – conductio rei*, *locatio – conductio operis* e *locatio conductio – operarum*.

---

<sup>24</sup> Cfr. DEMICHELIS L., *Bio-Tecnica. La società nella sua forma tecnica*, Napoli, 2008; DEMICHELIS L., *Il modello-panopticon. Dalla Nsa al Jobs Act*, su [www.temi.repubblica.it](http://www.temi.repubblica.it).

<sup>25</sup> Dagli usi aziendali, alla giurisprudenza probirale, dai primi concordati di tariffa alla legislazione sociale di fine secolo.

Sono le ultime due fattispecie a essere disciplinate nel primo codice civile del Regno di Italia. L'art. 1627 classificava tre specie di locazione di opere e di industria<sup>26</sup> e, in particolare, distingueva la *locatio operarum* dalla *locatio operis* stabilendo all'art.1628 che “nessuno può obbligare la propria opera all'altrui servizio che a tempo, o per una determinata impresa”.

Il dettato di tale ultima disposizione evidenziava uno dei tratti distintivi della *locatio operarum*, vale a dire la temporaneità, che andava di pari passo con la continuità, intesa come godimento nel tempo da parte del conduttore/datore di lavoro delle opere prestate da parte del locatore/lavoratore: quello che contava in questa fattispecie era il lavoro, non il risultato a cui la sua esplicazione portava, ciò che veniva enfatizzato era l'adempimento dell'obbligazione di un *facere*, adempimento diretto a soddisfare un interesse durevole del datore di lavoro, e dunque continuativo<sup>27</sup>.

Il contratto di locazione delle opere imponeva al *locator* di mettere a disposizione del *conductor* le proprie energie. Il contratto non trovava dunque il suo oggetto nella persona dell'uomo libero, bensì nelle energie lavorative, che potevano consistere sia nello svolgimento della prestazione lavorativa, che nel rimanere a disposizione del datore di lavoro. Tale contratto poneva a carico del lavoratore l'obbligo di compiere la propria attività in cambio di un corrispettivo, a cui era vincolato il datore di lavoro, tenuto a vigilare sul lavoro del primo.

“Il contratto di locazione delle opere risultava essere in sostanza la fattispecie corrispondente al moderno lavoro subordinato, in quanto il locatore doveva prestare la sua attività sotto il controllo e la direzione costante del conduttore”<sup>28</sup>.

Questo prova come, sin dal diritto romano, il creditore della prestazione, nella maggior parte dei rapporti contrattuali con oggetto un'obbligazione di *facere*, abbia interesse a verificare l'operato del debitore. Già all'epoca, era diffusa la concezione di un potere di controllo del datore di lavoro come un diretto effetto del potere direttivo, esercitato nei confronti dei dipendenti.

---

<sup>26</sup> Art.1627 c.c. 1865 “vi sono tre principali specie di locazione di opere e di industria: I – quella per cui le persone obbligano la propria opera all'altrui servizio; II – quella de' vetturini sì per terra come per acqua, che si incaricano del trasporto delle persone o delle cose; III – quella degli imprenditori di opere d'appalto o cottimo”.

<sup>27</sup> Cfr. MANNINO V., *Introduzione alla storia del diritto privato dei Romani*, Torino, 2011; SANTORO PASSARELLI G., *Diritto dei lavori e dell'occupazione*, Torino, 2017; PESSI R., *Lezioni di diritto del lavoro*, Torino, 2016; BIESUZ E., *Lavoro autonomo e subordinato: le posizioni in dottrina e giurisprudenza*, su [www.lavoroprevidenza.com](http://www.lavoroprevidenza.com) – Osservatorio di Diritto del Lavoro e di Previdenza Sociale, 31/05/2006 secondo i quali, il contratto di locazione d'opera determinava, invece, il sorgere dell'obbligo di eseguire un'opera o un servizio a carico di un *artifex*, che assumeva le vesti di conduttore, tenuto a realizzare e consegnare al creditore dell'opera, cioè il committente, gravato a sua volta dall'obbligo di pagare la mercede, il cd. *opus perfectum* concordato. In questa tipologia contrattuale l'oggetto del contratto non è dato dalle energie lavorative, ma da uno specifico risultato, quello che conta non è l'adempimento di un'obbligazione di mezzi o *facere*, ma l'adempimento di un'obbligazione di risultato, ciò che interessa non è il lavoro di per sé considerato, ma il compimento di un'opera con autonomia organizzativa.

<sup>28</sup> MANNINO V., op. cit..

La tesi del codice del 1865, per cui il contratto di lavoro doveva ritenersi una *species* del *genus* della locazione (*locatio operarum*), ha trovato un appoggio anche nel giurista e accademico italiano Lodovico Barassi.

Alla fine del secolo XIX la giurisprudenza, specie quella dei collegi probivirali, aveva individuato l'elemento atto a distinguere il rapporto di lavoro autonomo e subordinato nella disponibilità per il datore di lavoro del tempo del lavoratore, considerando l'inserimento e la dipendenza come modalità mediante le quali il datore di lavoro decide di impiegare il tempo del lavoratore. Questi concetti, nel 1901, sono stati ripresi da Barassi nella sua opera "il contratto di lavoro nel diritto positivo italiano" per costruire una nozione unitaria di subordinazione.

Nell'intento di Barassi, convinto dell'inseparabilità del lavoro dall'uomo<sup>29</sup>, vi è la riconduzione dello schema del lavoro subordinato al diritto civile, e tramite esso, alla tradizione romanistica. L'autore ha collegato la figura della *locatio operarum* al lavoro dipendente e quella della *locatio operis* al lavoro autonomo, rivalutando la portata dell'art. 1627 c.c. del 1865 e sottolineando l'elasticità e la adattabilità di tali concetti. Riteneva che il contratto di lavoro dovesse essere ricondotto allo schema unitario della locazione, definita come concessione a titolo oneroso del godimento delle energie provenienti da qualunque fonte, distinguendo tra *locatio operis* e *operarum*<sup>30</sup>. Nell'iniziare la sua distinzione tra le due tipologie contrattuali di matrice romanistica, Barassi sottolineava che a differenza della *locatio operis*, il lavoro tecnicamente subordinato ricordava il rapporto servile. E proprio dalla dipendenza innata nel rapporto servo – padrone, si originava la subordinazione della *locatio operarum*. La subordinazione del lavoratore rispetto al datore di lavoro era il tratto qualificante la locazione d'opere e si ricavava dalla circostanza che il lavoro era prestato sotto la guida e la responsabilità in proprio della persona a cui il lavoro era destinato, che si assumeva inoltre il rischio del lavoro. In primo piano vi erano da un lato le *operae*, per tale intendendosi l'attività svolta in sé indipendentemente dal risultato cui si mirava, e dall'altro l'accentramento della gestione del lavoro nel creditore del lavoro stesso<sup>31</sup>.

Gli indici di riconoscimento della subordinazione, ossia l'assunzione del rischio e l'accentramento della gestione del lavoro nella figura del del datore di lavoro, poiché privi di qualunque fondamento

---

<sup>29</sup> GRANDI M., "Il lavoro non è una merce": una formula da rimeditare, in *Lavoro e diritto*, 1997, afferma che Barassi, conservatore ma al tempo stesso consapevole degli eventi che stavano prendendo piede intorno a lui, abbia ritenuto necessario che il nascente diritto del lavoro fosse intriso dal dato dell'inseparabilità del lavoro dal lavoratore. All'epoca si trattava di qualcosa di più della semplice umanizzazione della *locatio hominis*, fermo restando che, sottolinea Grandi, nello schema della locazione le energie lavorative, date per non essere restituite, finivano per essere astratte dal corpo che le produce.

<sup>30</sup> SCOGNAMIGLIO R., *Contratto di lavoro e prestazione d'opere*, in NAPOLI M. (a cura di), *La nascita del diritto del lavoro, "Il contratto di lavoro" di Lodovico Barassi cent'anni dopo. Novità, influssi, distanze*, Milano, 2003.

<sup>31</sup> BARASSI L., *Contratto di lavoro nel diritto positivo italiano*, Roma - Milano - Napoli, 1915.

normativo, non permettevano all'epoca di considerare la subordinazione un dato di qualificazione giuridica dell'obbligazione lavorativa, cosa che avverrà invece con l'art. 2094 del codice civile del 1942.

Secondo Barassi, il lavoratore parte del rapporto di subordinazione, essendo inserito in un contesto lavorativo creato e diretto dal soggetto datoriale, è passivamente esposto a una unilaterale affermazione della volontà del creditore del lavoro, che risulta essere imperativa, come provano, ad es., gli ordini di servizio. Situazione che non si verifica invece nella *locatio operis*, in cui domina l'accentramento della gestione del lavoro, ovvero dell'autonomia del lavoro quanto all'elaborazione necessaria al conseguimento del risultato promesso nella figura del lavoratore. L'autore è consapevole del fatto che la grande industria abbia notevolmente contribuito all'elevazione delle classi lavoratrici e abbia impresso, rispetto al passato, dei *nova* anche nel contratto di lavoro, ma non ritiene che ciò sia sufficiente per innalzarlo a contratto di tipo autonomo dalla locazione di lavoro. Dunque, nonostante alla fine del secolo XIX, l'avvento della grande industria abbia reso evidente e, l'incompatibilità del contratto di locazione delle opere con la realtà che andava affermandosi e, la sua inidoneità a tutelare i lavoratori occupati nelle fabbriche, l'autore ha proseguito a considerare il contratto di lavoro appartenente alla categoria del contratto di locazione.

Questa sua linea di pensiero l'ha contrapposto alla giurisprudenza dell'epoca, sostenitrice della tesi dell'imprescindibile sottrazione del contratto di lavoro dal campo della locazione, facendo leva sull'affermazione sempre più vigorosa dell'importanza e della dignità che devono riconoscersi al lavoro umano; a differenza di quanto avveniva in passato le energie dell'essere umano non sono più equiparabili alle energie delle cose e degli animali, l'uomo non è più considerabile né definibile come una cosa bruta, con la conseguenza che il concetto di locazione non gli si addice.

#### **1.4 Il codice del 1942**

A cavallo dei secoli XIX e XX dunque, trovata il rapporto di lavoro una sua prima regolamentazione giuridica, si è passati dall'approccio di tipo formale del codice civile del 1865, che enfatizzava l'oggetto del contratto, contrapponendo le energie lavorative al risultato, a un approccio di tipo sostanziale, che si focalizzava sulla dipendenza del lavoratore dal datore di lavoro. L'impresa che si era andata cristallizzando era un'impresa gerarchica che trovava le sue fondamenta nell'assoggettamento del lavoratore agli ordini del datore di lavoro a fronte di un corrispettivo. Il lavoratore, quasi del tutto privo di tutele e diritti e spesso sovraccaricato di doveri e obblighi nei confronti del datore di lavoro, in tal modo era trasformato in un mero fattore di produzione a vantaggio di quest'ultimo.

Se bene o male si era consolidata nella cultura giuridica italiana l'inseparabilità del lavoro dal lavoratore prima della Grande Guerra, restava ancora molta strada da percorrere per inserire nel contratto il concetto di disuguaglianza sostanziale tra lavoratore e datore di lavoro e mettere l'accento sull'implicazione della persona nel rapporto di lavoro<sup>32</sup>: per acquisire cioè “*la consapevolezza che in materia di lavoro si scrive contratto ma si legge rapporto perché è nella corpulenta e prosaica realtà del rapporto che il lavoratore consuma un'esperienza di vita*”<sup>33</sup>.

Con l'entrata in vigore del codice del 1942 viene dedicata al lavoro una specifica disciplina: le disposizioni che lo riguardano, congiuntamente a quelle sull'impresa e sulla società, sono contenute nel Libro V. Questa è la fase dell'incorporazione del diritto del lavoro nel diritto privato, fase in cui si registra l'importante novità del distacco del contratto di lavoro subordinato dallo schema della *locatio*. Questo superamento ha rivelato il riconoscimento, da parte del nuovo codice civile, dell'implicazione della persona nello svolgimento del rapporto di lavoro. Il diritto del lavoro, che si ramifica in tre grandi aree<sup>34</sup>, diviene così lo strumento funzionale alla protezione del lavoratore subordinato e, essendo cristallina l'assenza di uguaglianza formale delle parti alle quali è ascrivibile la sottoscrizione del contratto di lavoro, e, essendo evidente la necessità di assicurare l'imparzialità dell'assetto negoziale, mediante interventi correttivi della disuguaglianza sostanziale delle parti.

Momento centrale è l'individuazione di quel contraente debole cui riferire l'apparato di tutele.

A riguardo, il codificatore del '42 si trovava di fronte due linee di pensiero, elaborate ormai compiutamente dalla dottrina italiana dopo il 1920, in ordine alla nozione di subordinazione che, concentrando l'attenzione sull'interesse del creditore-utilizzatore, piuttosto che sull'attività del debitore-locatore, si dividevano sull'alternativa se quell'interesse fosse soddisfatto con l'organizzazione del risultato produttivo determinato dall'attività del prestatore (e, quindi, se coincidesse con l'interesse dell'impresa oggettivamente considerata) o con la disponibilità senza aggettivi, e quindi generica, delle energie lavorative<sup>35</sup>.

L'oscillazione tra le due tesi ha spinto il codice del 1942 a sintetizzarle con l'inserimento dell'elemento della collaborazione nell'art. 2094 c.c..

---

<sup>32</sup> Cfr. BALLESTRERO M.V., *Le “energie da lavoro” tra soggetto e oggetto*, in WP C.S.D.L.E. “Massimo D’Antona” .IT - 99/2010; CANESTRARI S. – FERRANDO G. - MAZZONI C.M. – RODOTÀ S. – ZATTI P. (a cura di), *Trattato di biodiritto. Il governo del corpo*, Milano, 2011.

<sup>33</sup> ROMAGNOLI U., *Il lavoro in Italia*, Bologna, 1995.

<sup>34</sup> Tradizionalmente il diritto del lavoro si ripartisce in: diritto del lavoro in senso stretto, comprendente la materia oggetto del contratto e del rapporto di lavoro; diritto sindacale, inerente la disciplina dei rapporti sindacali, la contrattazione collettiva e l'autotutela sindacale; e infine la legislazione sociale, concernente le norme regolatrici dei rapporti tra lo Stato, datori e prestatori di lavoro, e le norme in materia di previdenza e assistenza sociale.

<sup>35</sup> PESSI R., *Lezioni di diritto del lavoro*, Torino, 2016.

L'art. 2094 c.c. qualifica come prestatore di lavoro subordinato “*chi si obbliga mediante retribuzione a collaborare nell'impresa, prestando il proprio lavoro intellettuale o manuale alle dipendenze e sotto la direzione dell'imprenditore.*”

Secondo la concezione tradizionale, la subordinazione, elemento tipizzante il rapporto di lavoro dipendente, viene identificata dalla disposizione nella collaborazione del lavoratore alle dipendenze e sotto la direzione dell'imprenditore. Queste ultime due espressioni sono la manifestazione di due profili differenti della subordinazione.

Dire che il prestatore di lavoro si trova *alle dipendenze* del suo datore di lavoro significa dire che il dipendente, una volta assunta l'obbligazione scaturente dalla sottoscrizione del contratto, in quanto alle dipendenze dell'imprenditore, agisce nell'interesse del datore di lavoro.

L'espressione “*sotto la direzione*” indica che l'imprenditore, stabilite le modalità di esecuzione della prestazione nel momento costitutivo del rapporto di lavoro, ha il potere di modificarle in un secondo momento.

Si parla di subordinazione tecnico – funzionale. Tale nozione fa riferimento al carattere dell'etero-determinazione della prestazione, nel senso che il lavoratore subordinato esegue la prestazione dedotta in contratto secondo ordini, direttive e impostazioni impartite dal datore di lavoro, con cui si determina concretamente l'attività da svolgere e in capo al quale vengono tradizionalmente riconosciuti i tre poteri che hanno la loro causa giustificatrice nello squilibrio tra le parti, elemento insito del rapporto subordinato. Si tratta del potere di controllo, direttivo e disciplinare<sup>36</sup>.

In tal senso è in seguito intervenuto lo Statuto dei lavoratori del 1970 ponendo un argine all'esercizio dei poteri imprenditoriali, in particolare, nel titolo I, con le norme rivolte alla tutela della “Libertà e dignità del lavoratore”, proprio a conferire rilievo all'implicazione giuridica della persona del lavoratore nell'attuazione del rapporto.

Il concetto di subordinazione tecnico – funzionale, cui si aggiunge quella socio-economica per indicare la dipendenza economica del lavoratore dal datore di lavoro, è simmetricamente ribadita dall'art. 2222 c.c. quando definisce il lavoratore autonomo come colui che opera “*senza vincolo di subordinazione nei confronti del committente*”, organizzando dunque liberamente la propria attività. E nonostante la giurisprudenza abbia elaborato nel corso degli anni molteplici indici<sup>37</sup> volti a facilitare la distinzione tra lavoro autonomo e subordinato, essi mantengono un rilievo secondario

---

<sup>36</sup> Cfr. MAZZOTTA O., *Diritto del lavoro*, Milano, 2013; SANTORO PASSARELLI G., *Diritto dei lavori e dell'occupazione*, Torino, 2017.

<sup>37</sup> Si tratta dell'osservanza di un orario di lavoro predeterminato, della collaborazione, dell'assenza del rischio in capo al lavoratore, della natura e della continuità della prestazione, del versamento di una retribuzione prestabilita a cadenze fisse, dell'inserimento del lavoratore nell'organizzazione produttiva, del coordinamento dell'attività lavorativa all'assetto organizzativo dato all'impresa dal datore di lavoro. Cfr. per l'affermazione della loro natura sussidiaria e non

rispetto all'unico elemento avente valore determinante per dimostrare l'esistenza del vincolo di subordinazione: l'assoggettamento del lavoratore al potere di direzione e di controllo del datore di lavoro<sup>38</sup>.

Lo schema locativo viene dunque sepolto dall'art. 2094 c.c. che ha tipizzato la subordinazione come criterio di qualificazione del contratto<sup>39</sup>.

### **1.5 La Costituzione e la normativa sovranazionale**

Il momento più significativo di sviluppo della tutela di cittadini e lavoratori, è rappresentato dalla Costituzione repubblicana del 1947, a cui si riconosce il merito di aver avviato una nuova stagione del diritto del lavoro, la fase della costituzionalizzazione.

Nell'ambito del progetto costituzionale di elevazione della persona umana, il rapporto tra privati di maggior rilievo diviene proprio quello di lavoro e, in particolare, quello di lavoro subordinato. Sancendo all'art. 1 che la Repubblica è fondata sul lavoro, la Costituzione ha sostituito la visione democratica e sociale a quella corporativistica dello stato fascista, visione quest'ultima in cui la libertà non assurgeva a valore fondamentale nell'ordinamento e in cui il lavoratore era fattore di produzione esplicitante il dovere sociale di lavoro, essendo considerato il lavoro stesso come attività dedicata non allo scopo economico proprio del datore di lavoro, come in epoca di rivoluzione industriale, ma allo scopo produttivo di rilevanza nazionale.

La Costituzione assicura un sistema di tutele giuslavoristiche su due livelli<sup>40</sup>. In primis, sul piano dei principi fondamentali, bisogna far riferimento a una serie di altre norme, oltre al menzionato art. 1: l'art. 35 Cost. che tutela *"il lavoro in tutte le sue forme ed applicazioni"*, anche all'estero, e cura *"la formazione e l'elevazione professionale dei lavoratori"*; l'art. 36 Cost. che, assicurando la c.d. tutela retributiva, eleva a rango di principi costituzionali i diritti, già riconosciuti dal codice civile del 1942 e dalla legislazione speciale, a un limite massimo di ore di lavoro, al riposo settimanale e a ferie annuali retribuite e irrinunciabili; l'art. 37 Cost. si occupa della tutela delle donne e dei minori, riconoscendo alla donna lavoratrice parità di diritti e il diritto all'assolvimento delle sue funzioni familiari e materne e stabilendo la necessità di un limite minimo di età per lo svolgimento dell'attività lavorativa; l'art. 38 Cost., configurando la c.d. sicurezza sociale, assicura che ogni

---

decisiva, Cass., 21 febbraio 2006, n.4171, su <http://www.dirittolavoro.org/>; Cass., 2 maggio 2012, n. 6643, su <http://adapt.it/>.

<sup>38</sup> Cfr. Cass., 21 febbraio 2006, n. 4171, su <http://www.dirittolavoro.org/>; Cass., 8 febbraio 2010, n. 2728, in Arg. Dir. Lav., 2010, p. 943.; Cass., 19 aprile 2010, n. 9215, su <https://www.diritto.it/> con nota di MARAGA R.; Cass., 10 marzo 2011, n. 5712, su <http://www.gadit.it/>; Cass., 2 maggio 2012, n. 6643, su <http://adapt.it/>.

<sup>39</sup> MENGONI L., *L'evoluzione del pensiero di L. Barassi dalla prima alla seconda edizione del "contratto di lavoro"*, in Id. *Il contratto di lavoro* di NAPOLI M., Milano, 2004.

<sup>40</sup> MORTATI C., *Commento all'art. 1 della Costituzione*, in *Commentario della Costituzione*, BRANCA C. (a cura di), 1° Vol., Artt. 1-12: principi fondamentali, Bologna, 1975.

lavoratore abbia mezzi adeguati alle esigenze di vita in caso di infortunio, malattia, invalidità, vecchiaia e disoccupazione<sup>41</sup>; gli artt. 39 e 40 Cost. infine sanciscono rispettivamente che l'organizzazione sindacale è libera e il diritto di sciopero.

In secundis, nell'alveo del Titolo V della Costituzione, a seguito della legge costituzionale n. 3 del 2001, si deve far riferimento all'art. 117 Cost.: tale disposizione rovescia il criterio di ripartizione tra le materie di competenza dello Stato e delle Regioni mediante un elenco delle materie soggette alla legislazione statale o regionale nel rispetto dei principi fondamentali<sup>42</sup>.

Per una ricostruzione completa delle linee direttrici fondamentali del diritto del lavoro, però, non può farsi unico riferimento al testo della Carta costituzionale italiana, ma è utile richiamare anche i principi espressi a livello sovranazionale. La fine del secondo conflitto mondiale aveva prodotto una spinta crescente nella tutela dei diritti inviolabili dell'uomo e del cittadino, così configurando un'emersione dei c.d. diritti sociali, fonte del libero svolgersi della personalità umana, tra cui rientra il diritto al lavoro e alla formazione professionale<sup>43</sup>. Sul piano internazionale, la tutela dell'uomo che lavora e la volontà di evitarne lo sfruttamento costituiscono l'obiettivo principale della c.d. Organizzazione internazionale del lavoro (OIL), di cui fanno parte tutti gli stati membri delle Nazioni Unite. Tuttavia, nell'ordinamento italiano, un'influenza maggiore rispetto a quella esercitata dagli atti dell'OIL è assunta dalla normativa comunitaria, i cui principi fondamentali sono oggi espressi nel Trattato di Lisbona del 13 dicembre 2007. In particolare l'art. 153 TFUE decreta, come principali obiettivi da raggiungere in ambito di diritto del lavoro, tra gli altri, il miglioramento dell'ambiente di lavoro a tutela della sicurezza e della salute dei lavoratori, la sicurezza sociale e protezione sociale dei lavoratori, la rappresentanza e la difesa collettiva degli interessi dei lavoratori e dei datori di lavoro.

## **2. Il datore di lavoro e i suoi poteri**

Concluso questo breve excursus normativo si può ora passare all'analisi dei poteri datoriali. Con la sentenza del 2 maggio 2012 n. 6643 la Corte di Cassazione ha sancito che *“ai fini della distinzione del rapporto di lavoro subordinato da quello autonomo, costituisce requisito fondamentale il vincolo di soggezione del lavoratore al potere direttivo, organizzativo e*

---

<sup>41</sup> NAPOLI M., *Le norme costituzionali sul diritto del lavoro alla luce dell'evoluzione del diritto del lavoro*, in Scritti in onore di Edoardo Ghera, Bari, 2008.

<sup>42</sup> L'ordinamento civile, tra cui vi rientra il rapporto individuale di lavoro e il diritto sindacale nella sua dimensione privatistica, appartiene alla competenza esclusiva della legislazione statale ai sensi del secondo comma lett. l) dell'art. 117 Cost.

<sup>43</sup> PESSI R., *Lezioni di diritto del lavoro*, Torino, 2016.

*disciplinare del datore di lavoro, il quale discende dall'emanazione di ordini specifici, oltre che dall'esercizio di una assidua attività di vigilanza e controllo dell'esecuzione delle prestazioni lavorative*<sup>44</sup>.

Il datore di lavoro, con la sottoscrizione del contratto, è legittimato a esercitare i suoi poteri nei confronti del lavoratore assunto. L'esercizio di tali poteri, che hanno la loro fonte nel rapporto contrattuale, è spesso regolato dalla legge, giacché il legislatore è progressivamente intervenuto sugli stessi, limitando il loro esercizio (es. il potere di licenziamento) o procedimentalizzandone l'utilizzo (es. il potere disciplinare).

## **2.1 Il potere di controllo**

La fonte del rapporto di lavoro è il contratto e non l'immissione del lavoratore in un'istituzione ordinata su base gerarchica.

La vicenda contrattuale si articola in diverse fasi che si susseguono: il contratto nasce con l'accordo, vive la sua vita con l'esecuzione della prestazione e si estingue o naturalmente (per scadenza del termine o per adempimento) o, in modo patologico, e cioè a causa del proficuo esperimento dei rimedi messi a disposizione delle parti contrattuali dal legislatore (risoluzione, recesso, mutuo consenso, invalidità). Il potere di controllo in questa sequenza temporale svolge un ruolo da protagonista: costituisce lo strumento che il creditore della prestazione ha a sua disposizione per verificare il soddisfacimento del proprio interesse o, al contrario, in caso d'inesatta o addirittura assente prestazione del debitore, costituisce preconditione per il valido esperimento dei rimedi che portano all'estinzione del contratto. Infatti, con l'esercizio del potere di controllo il creditore non solo acquisisce informazioni circa il corretto svolgimento dell'opera, ma si assicura anche le prove dell'inesatta esecuzione, che potrà far valere a sostegno della sua pretesa in un eventuale successivo giudizio. L'esigenza di verificare l'operato del debitore si avverte in particolar modo nel rapporto di lavoro subordinato. Il lavoratore, infatti, per svolgere esattamente la sua prestazione si trova inserito in un'organizzazione di mezzi e di uomini a lui estranea, ma alla quale deve conformarsi. La specialità della vicenda contrattuale in esame, infatti, è data dalla continua e costante soggezione del debitore al potere direttivo del creditore, che a proprio rischio *“programma, organizza e dirige l'apparato in cui s'inserisce il debitore con la sua attività e, sovente, con la sua persona”*<sup>45</sup>.

Quindi il lavoratore subordinato è destinatario delle disposizioni e delle direttive impartite dal datore di lavoro per realizzare le finalità di quest'ultimo e, correlativamente, soggiace al controllo

---

<sup>44</sup> Cass., 2 maggio 2012, n. 6643, su <http://adapt.it/>.

<sup>45</sup> GHEZZI G. – ROMAGNOLI U., *Il rapporto di lavoro*, Bologna, 1987.

creditorio sulla conformazione del suo operato alle direttive ricevute nonché ai parametri di cui all'art. 2104 c.c.<sup>46</sup>.

La vigorosa implicazione della persona del lavoratore nello svolgimento dell'attività lavorativa, espressa per la prima volta dal codice civile del 1942, espone al pericolo che il controllo del datore di lavoro venga esercitato in modo da diventare atto lesivo della dignità e della riservatezza del lavoratore stesso. Nessuna norma del codice civile menziona il potere di controllo, per ottenerne un esplicito riconoscimento bisognerà attendere la l. 300/1970 (Statuto dei lavoratori, in seguito St. lav.) che, per la prima volta, con il suo articolo 4, regolerà manifestamente, il potere del datore di lavoro di controllare a distanza l'attività lavorativa, in quanto strumentale alla realizzazione del suo interesse tecnico – organizzativo, fissandone allo stesso tempo i limiti proprio a protezione della sfera personale del prestatore di lavoro<sup>47</sup>.

All'interno del rapporto di lavoro subordinato, in cui da un lato vi sono i poteri del datore di lavoro e dall'altro i diritti del lavoratore, il potere di controllo riveste notevole importanza per il datore perché il suo esercizio gli consente di sorvegliare i lavoratori, potenzialmente *cotidie et singulis momentis*, per verificare che adempiano correttamente e diligentemente la prestazione dedotta nel contratto.

Sotto questo profilo, secondo una parte della dottrina, il potere di controllo è tradizionalmente considerato come una componente naturale del potere direttivo, in quanto consente al datore di lavoro di accertare il rispetto delle indicazioni da lui impartite al lavoratore nell'espletamento delle mansioni<sup>48</sup>. È strettamente inerente alla figura dell'imprenditore giacché 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 dentro l'impresa.

Perché l'esercizio di tale potere sia legittimo è necessario che avvenga nel rispetto della dignità e della riservatezza dei lavoratori. Verso la metà del secolo scorso era quasi all'ordine del giorno l'esigenza di limare quella disuguaglianza tra le parti contrattuali ancora fortemente presente: nonostante il registrato miglioramento della posizione del lavoratore, non più del tutto privo di diritti grazie all'avvento della Costituzione repubblicana del 1947, era ancora necessario

---

<sup>46</sup> Cfr. VENEZIANI B., *I controlli dell'imprenditore ed il contratto di lavoro*, Bari, 1975; DE LUCA TAMAJO R., *I Controlli sui lavoratori*, in ZILIO GRANDI G. (a cura di), *I poteri del datore di lavoro nell'impresa*, Atti del Convegno di studi, Venezia, 2003, il quale mette in luce che il datore ha interesse all'informazione e al controllo e che tali esigenze nella logica dialettica tipica del diritto del lavoro si contrappongono al diritto alla riservatezza del lavoratore.

<sup>47</sup> CARINCI M.T., *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.Lgs. 151/2015): spunti per un dibattito*, in *Labour & Law Issues*, vol. 2, no. 1, 2016.

<sup>48</sup> BARRACO E. – STIZIA A., *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milanofiori Assago (MI), 2016.

contemperare le esigenze di tutela del prestatore di lavoro con le esigenze datoriali, dovendosi riconoscere a entrambe pari dignità giuridica. La necessità di arginare l'esercizio dell'invasivo potere di controllo era in prima linea, a maggior ragione tenuto conto dell'origine del diritto del lavoro, tradizionalmente nato e sviluppatosi, come visto, a tutela del lavoratore subordinato, soggetto dipendente economicamente e giuridicamente dal datore di lavoro.

Infine ultimo aspetto da evidenziare è che l'esercizio del potere di controllo per la verifica della corretta esecuzione della prestazione lavorativa e del rispetto delle disposizioni impartite è legato alla libertà di iniziativa economica e non può svolgersi in violazione della libertà e dignità umana, cioè in violazione di quanto prescritto all'art. 41, comma 2, della Costituzione.

*“A fronte dei nuovi epicentri della crisi-trasformazione indotti dalle nuove tecnologie e dalla globalizzazione, si è aperta una nuova stagione del Diritto del lavoro che deve, ormai, tenere conto del riconoscimento costituzionale della libertà di iniziativa economica, il quale comporta l'accettazione di un sistema di economia di mercato e, quindi, impone al giurista una sintesi di razionalità tra i valori della persona ed i valori dell'economia”*<sup>49</sup>.

L'articolo 41 della Costituzione prevede al primo comma che *“l'attività economica privata è libera”*.

La libertà di iniziativa economica sembra ricomprendere, nell'opinione più diffusa, e, la libertà dell'impresa di decidere se intraprendere un'attività economica, e, quella di organizzarla: la libertà di iniziativa economica diventa la libertà di decidere che cosa, quanto, come e dove produrre. L'art. 41, comma 1, Cost. tutela sia la fase propulsiva, sia la fase di svolgimento dell'attività economica. La conseguenza di ciò è che i limiti, entro il cui rispetto può svolgersi attività economica, dettati dall'art. 41, comma 2, Cost., sono comuni a entrambe le fasi in cui si sviluppa l'attività economica<sup>50</sup>.

L'art. 41, comma 2, Cost. prevede che l'iniziativa economica privata *“non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana”*. Secondo l'orientamento prevalente, i limiti posti da tale secondo comma rappresentano un limite “esterno” e non già un limite interno all'attività economica. L'utilità sociale è un limite esterno, non un limite funzionale, non è un fine determinante la legittimità dell'iniziativa economica: se lo fosse ci sarebbe un contrasto con quanto prescritto nel primo comma, si nega dunque la funzionalizzazione dell'iniziativa economica privata all'utilità sociale. Da un lato, questo evidenzia come, con il suo dettato, la disposizione in esame non intenda

---

<sup>49</sup> PESSI R., *Impresa e diritto del lavoro*, in Gnosis – Rivista italiana di Intelligence 4/2008.

<sup>50</sup> COSTANTINI S., *Limiti all'iniziativa economica privata e tutela del lavoratore subordinato: il ruolo delle cd. “clausole sociali”*, in Ianus - Diritto e Finanza n. 5/2011, pp. 203-204.

assoggettare l'attività dell'imprenditore a esigenze di natura pubblicistica o a interessi alieni rispetto a quelli dell'imprenditore stesso: quest'ultimo ha diritto di costituire l'impresa per perseguire un proprio profitto e la legge ordinaria non può impedirlo. L'art. 41 Cost. riconosce il fatto che, in quanto svolta all'interno di una società fatta di valori, principi ed esigenze, l'attività economica deve essere attuata nel loro rispetto. Partendo da questo assunto, il legislatore ha attribuito al datore di lavoro i poteri di cui si discute, affinché lo svolgimento dell'attività economica potesse effettivamente portare alla realizzazione degli obiettivi per la quale è stata avviata, poteri assolutamente necessari affinché l'imprenditore possa mantenere il controllo dell'attività<sup>51</sup>.

Dall'altro lato, l'utilità sociale dell'impresa non può essere ignorata. Essa deve essere intesa come espressione dei bisogni della comunità e della sua funzione, strettamente collegata all'interesse alla conservazione e alla crescita dell'occupazione, quale garanzia dell'effettività del diritto al lavoro. L'utilità sociale è quindi coerente con gli interessi della "maggioranza sociale"; ma per realizzare la sua funzione essa deve trovare concretizzazione anche nell'economicità e produttività dell'iniziativa privata. Al pari della sicurezza, dignità e libertà umana rappresentano una sorta di contenitore che necessita essere riempito di contenuto normativo dal legislatore, espressione del principio democratico della maggioranza, come si è verificato con varie leggi in materia di lavoro e soprattutto con la l. n. 300/1970. Questo implica che i poteri dell'imprenditore possono progressivamente incontrare dei limiti posti loro dalla legge e dalla contrattazione collettiva, fermo restando che, come detto, queste ultime non possono mai funzionalizzare l'esercizio all'utilità sociale.

Si apre così una nuova fase della vita del diritto del lavoro, quella di cui parla Mattia Persiani, quella che deve, oramai, tener conto del riconoscimento costituzionale della libertà di iniziativa economica, riconoscimento che implica l'accettazione di un sistema di economia di mercato con la conseguenza che anche l'impresa è un valore costituzionale, oltre che economico<sup>52</sup>.

*“È un salto di qualità. L'impresa non è soltanto luogo di produzione del profitto capitalistico, ma è anche oggetto di attese sociali, divenendo così strumento per la realizzazione dei valori della persona. Essa non deve essere considerata soltanto “una società di capitali” ma anche, secondo il pensiero di Giovanni Paolo II nell'enciclica “Centesimus Annus”, “una società di persone di cui entrano a far parte in modo diverso e con specifiche responsabilità, sia coloro che forniscono il capitale necessario per la sua attività, sia coloro che vi collaborano con il proprio lavoro”. Proprio per soddisfare queste attese l'impresa deve produrre ricchezza e, quindi, dovendosi*

---

<sup>51</sup> COSTANTINI S., ibidem.

<sup>52</sup> SANTORO PASSARELLI G. op.cit.

*confrontare con il mercato, deve necessariamente perseguire obiettivi di efficienza e produttività*<sup>53</sup>.

## **2.2 Il potere direttivo**

Sebbene il potere di controllo sia largamente considerato una prosecuzione naturale del potere direttivo, secondo autorevole dottrina<sup>54</sup> in realtà è un potere distinto dal potere direttivo, perché è destinato alla verifica dell'esatto adempimento dell'obbligazione lavorativa e perché è limitato da norme dello Statuto differenti da quelle che regolano l'esercizio del potere direttivo. Infatti, diversamente da queste ultime, sono poste a garanzia della dignità e riservatezza del lavoratore.

Il potere direttivo, in quanto tale, trova particolare fondamento nell'art. 2104, comma 2, c.c., secondo cui il prestatore di lavoro “*deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende*”. Tramite l'esercizio del potere direttivo, dunque, datore di lavoro e collaboratori fissano le modalità di esecuzione e i tempi della prestazione lavorativa, precisando come debba essere adempiuta l'obbligazione scaturente dal contratto di lavoro per il lavoratore, affinché sia fruttuosa per il raggiungimento degli scopi prestabiliti. L'esercizio del potere direttivo permette di fissare disposizioni regolatrici della prestazione lavorativa, in modo tale da ottenere la migliore funzionalizzazione delle energie psico – fisiche del lavoratore al conseguimento degli obiettivi produttivi.

Ai sensi dell'art. 2103 c.c., nel testo novellato dal d.lgs. n. 81 del 2015, il datore di lavoro ha il potere di adibire il lavoratore “*alle mansioni per le quali è stato assunto o a quelle corrispondenti all'inquadramento superiore che abbia successivamente acquisito ovvero a mansioni riconducibili allo stesso livello e categoria legale di inquadramento*”.

La novità che il d.lgs. n. 81 del 2015 ha apportato al primo comma è la sostituzione della regola dell'equivalenza con quella della categoria e del livello di inquadramento. Nell'originario testo dell'art. 2103 c.c., la regola dell'equivalenza consentiva al datore di adibire il lavoratore a mansioni diverse, a patto che le mansioni di nuova adibizione fossero equivalenti alle precedenti. L'equivalenza era ravvisata se le nuove mansioni fossero rientrate nello stesso livello di inquadramento e avessero consentito la conservazione della professionalità acquisita, vale a dire l'uso da parte del lavoratore di quanto già appreso, a livello di esperienza, perizia o nozioni, nella fase pregressa del rapporto di lavoro.

---

<sup>53</sup> PESSI R., *Impresa e diritto del lavoro*, in *Gnosis – Rivista italiana di intelligence* 4/2008.

<sup>54</sup> SANTORO PASSARELLI G., op. cit.

Altra novità registrata alla luce del nuovo testo è che, non è più soltanto legittimo lo *jus variandi in melius*, la cui disciplina è stata sostanzialmente mantenuta, ma è legittima anche l'adibizione del lavoratore a mansioni inferiori, a due condizioni che fungono da presupposto di legittimità dell'esercizio dello *jus variandi in peius*: vi deve essere una modifica degli assetti organizzativi che incide sulla posizione del lavoratore e le mansioni inferiori devono rientrare nella medesima categoria legale<sup>55</sup>.

Il potere direttivo del datore di lavoro, infine, tramite fonti legali o a volte negoziali, è stato più volte sottoposto a una serie di limiti: negativi o positivi (che impongono un obbligo di fare o di non fare), finali o procedimentali (i primi vietano o impongono determinati atti in modo da definire la fattispecie sostanziale, i secondi condizionano l'esercizio del potere datoriale al previo espletamento di determinate procedure di carattere sindacale o amministrativo) o ancora interni o esterni (tra i primi si ricorda l'obbligo di giustificare un licenziamento, tra i secondi la necessità del nulla osta del sindacato di appartenenza per il trasferimento del dirigente sindacale aziendale) e infine a efficacia reale o obbligatoria<sup>56</sup>.

### **2.3 Il potere disciplinare**

L'esercizio del potere di controllo, fungendo da costante occhio vigile sull'attività del prestatore di lavoro, permette inoltre al datore di prendere contezza, all'istante, della commissione di un'infrazione presente nel codice disciplinare a opera del lavoratore. In questo senso, il potere di controllo risulta essere funzionalizzato all'esercizio del potere disciplinare, in quanto il datore procederà all'esercizio del potere sanzionatorio nei confronti del lavoratore, reo della violazione riscontrata, al fine di irrogare la dovuta sanzione.

Il potere disciplinare è un potere di cui gli imprenditori si sono dotati sin dall'inizio della rivoluzione industriale nei confronti dei loro dipendenti e che esercitavano arbitrariamente, senza attendere che trovasse esplicito riconoscimento nelle leggi o nei contratti collettivi. La dottrina e la giurisprudenza consideravano legittima l'operatività del potere in assenza di una preventiva esplicitazione a livello legislativo o in un regolamento aziendale, a patto che fosse rispettata la regola generale della proporzionalità tra la sanzione disciplinare, vista in tale contesto come pena personale, e la gravità della mancanza commessa dal lavoratore.

Il primo riconoscimento del potere si deve alla Carta del lavoro approvata dal Gran Consiglio Fascista il 21 aprile 1927, a norma della quale "*le infrazioni alla disciplina e gli atti che perturbino*

---

<sup>55</sup> PISANI C., *La nuova disciplina del mutamento delle mansioni*, Torino, 2015.

<sup>56</sup> PESSI R., *Lezioni di Diritto del lavoro*, Torino, 2016.

*il normale andamento dell'azienda, commessi dai prenditori di lavoro, sono puniti, secondo la gravità della mancanza, con la multa, con la sospensione del lavoro e, per i casi più gravi, col licenziamento immediato senza indennità*” (XIX dichiarazione, primo comma); con l'aggiunta che *“saranno specificati, ma non si precisa in quale sede e in quale forma, i casi in cui l'imprenditore può infliggere la multa o la sospensione o il licenziamento immediato senza indennità”* (secondo comma)<sup>57</sup>.

Il fondamento normativo del potere disciplinare è l'art. 2106 c.c. . Da tale disposizione si ricava che l'esercizio del potere in esame permette al datore di lavoro di reagire all'eventuale inadempimento del lavoratore, reo di violazione degli obblighi di diligenza e fedeltà su di lui gravanti, consacrati rispettivamente negli artt. 2104 comma 1 e 2105 c.c.: l'obbligo di diligenza impone al lavoratore di usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello della produzione nazionale; l'obbligo di fedeltà prescrive al lavoratore di non trattare affari in concorrenza con l'imprenditore o di non fare uso di notizie inerenti all'organizzazione e i modi di produzione dell'impresa per arrecarvi danno. L'esercizio del potere disciplinare consente al datore di lavoro di punire l'inosservanza di tali obblighi senza compromettere la conservazione e la continuità del rapporto di lavoro. Conservazione che in alcuni casi soddisfa le esigenze imprenditoriali in misura maggiore rispetto all'interruzione del rapporto.

L'art. 2106 c.c. pone inoltre all'esercizio del potere disciplinare un limite, dettato dalla regola della proporzionalità tra entità dell'infrazione e misura della sanzione, dovendo quest'ultima essere proporzionata alla gravità del fatto contestato e accertato a carico del lavoratore. A integrazione di ciò, l'art. 7 St. lav. ha introdotto diversi principi e garanzie dirette a ridurre l'esercizio arbitrario del potere disciplinare, che è andato a procedimentalizzarsi. In particolare ha immesso il principio di legalità, stabilendo che il codice disciplinare aziendale, da portare a conoscenza del lavoratore mediante affissione in luogo accessibile a tutti, debba indicare le infrazioni e le sanzioni a esse corrispondenti, richiamando quanto è previsto dal contratto collettivo. L'art. 7 St. lav., accanto al principio di legalità delle infrazioni e delle sanzioni, ha poi introdotto il principio del contraddittorio, che obbliga il datore di lavoro alla contestazione della condotta concedendo al responsabile la possibilità di presentare memorie difensive per iscritto e di essere ascoltato personalmente prima dell'irrogazione della sanzione. Il lavoratore può chiedere entro venti giorni dalla comunicazione della sanzione la costituzione di un collegio di conciliazione e di arbitrato, i cui atti hanno natura negoziale. La sanzione resta sospesa fino alla definizione del lodo che può non solo confermare, ma anche modificare la specie e l'entità della sanzione. La sanzione resta

---

<sup>57</sup> ICHINO P., *Lezioni di Diritto del lavoro*, Milano, 2004.

parimenti sospesa fino alla definizione del giudizio nell'ipotesi in cui il datore di lavoro non intenda aderire alla procedura arbitrale e domandi al giudice l'accertamento della legittimità della sanzione irrogata. La sanzione diventa inefficace se il datore di lavoro non provvede, entro dieci giorni, alla nomina del proprio arbitro.

Infine in caso di recidiva, si configura a carico del dipendente una responsabilità disciplinare connotata da gravità maggiore, data l'intenzione del lavoratore di eludere sistematicamente l'obbligo di una corretta prestazione<sup>58</sup>.

### **3. Il controllo a distanza nella versione originaria dell'art. 4 dello Statuto dei lavoratori**

Un primo passo rivolto alla conquista del bramato bilanciamento tra l'interesse del lavoratore alla tutela della propria sfera riservata e l'interesse del datore di lavoro al controllo, strumentale a un'ottimale organizzazione del proprio ciclo produttivo, è stato compiuto dallo Statuto dei lavoratori, in cui domina l'immagine del lavoratore subordinato come di un soggetto titolare di diritti fondamentali della persona. Tale riconoscimento è il traguardo del breve excursus storico-normativo percorso in precedenza.

Anticipando di molto il Codice della privacy e rispondendo a specifiche esigenze di protezione della persona del lavoratore, inserita in un contesto soggetto a regole di potere, ove è esposta alla compressione delle libertà e dignità personali<sup>59</sup>, la normativa statutaria ha limitato l'ammissibilità dei cd. "controlli umani" sulla prestazione lavorativa e reso non legittima la raccolta di informazioni non funzionali al rapporto di lavoro, vietando gli accertamenti datoriali. Il controllo sull'espletamento delle mansioni è attuabile, oltre che mediante soggetti a ciò specificatamente adibiti<sup>60</sup>, tramite l'installazione di impianti audiovisivi e, a oggi, di altri strumenti. L'art. 4 dello Statuto dei lavoratori riveste una notevole importanza perché, insieme alle disposizioni concernenti il controllo umano, *"fa parte di quella complessa normativa diretta a contenere in vario modo le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti nella sfera interna della persona, si ritengono lesive della dignità e della riservatezza del lavoratore"*<sup>61</sup>.

Nella relazione al d.d.l. Statuto dei lavoratori del Ministro Giacomo Brodolini si legge *"la salvaguardia della libertà e dignità, umana e sociale, del lavoratore, nella sua duplice qualità di*

---

<sup>58</sup> BUFFA F. – DE GIORGI C., *Il potere disciplinare. Nel lavoro privato, nel lavoro pubblico contrattualizzato, nel pubblico impiego e nel settore militare*, Matelica (MC), 2007.

<sup>59</sup> BALLESTRERO M.V. – DE SIMONE G., *Diritto del lavoro*, Torino, 2017.

<sup>60</sup> Artt. 2 e 3 St. lav.

<sup>61</sup> Cass., 17 giugno 2000, n.8250, su <https://www.unioncamere.gov.it/>; Cass., 17 luglio 2007, n. 15892, in Riv. It. Dir. Lav., 2008, n. 3, II, pp. 714 ss., con nota di VALLAURI M.L.

*cittadino e di parte del rapporto di lavoro, non potrebbe ritenersi compiutamente realizzata da una normativa che si esaurisca nella garanzia di una attiva presenza del sindacato nel luogo di lavoro. (...) il titolo primo della presente legge vuole assicurare ai lavoratori l'effettivo godimento di taluni diritti e libertà fondamentali che, pur trovando nella Costituzione una disciplina e una garanzia complete sul piano dei principi, si prestano tuttavia, in carenza di disposizioni precise di attuazione, ad essere compressi nel loro libero esercizio. Queste considerazioni giustificano e, al tempo stesso, impongono le disposizioni contenute nel Titolo I.”*

La norma dunque intendeva e, ridurre l'impegno di lavoro nei limiti di una certa tollerabilità o lassismo, senza esasperazioni stacanovistiche e, impedire che, attraverso la legittimazione del controllo del datore di lavoro sull'adempimento dell'obbligazione lavorativa, si producesse un controllo di carattere personale, sulla persona fisica o psichica del lavoratore, evitando cioè che il lavoratore, nel conferire le proprie energie lavorative, esponesse a controllo anche la propria persona, la propria riservatezza, la propria dignità<sup>62</sup>.

L'art. 4 St. lav., nonostante alcune incertezze interpretative, non solo costituisce il punto di riferimento normativo essenziale per la disciplina delle forme di controllo a distanza realizzabili mediante apparecchiature elettroniche, ma ha anche fronteggiato la mancanza nel nostro Paese, registratasi fino al 2003, di una regolamentazione generale sul trattamento dei dati personali, sentita come dovuta in ragione del problema originato dall'avvento delle nuove tecnologie, ossia quello della possibilità, per il datore di lavoro, di acquisire e trattare dati personali per gli scopi più disparati<sup>63</sup>.

### **3.1 I controlli intenzionali**

Coerentemente con la realtà di cui era frutto, l'art. 4 dello Statuto dei lavoratori presentava un testo piuttosto lineare sancendo, nel primo comma, che “è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori”.

Mentre il controllo umano era ammesso nel rispetto di alcuni limiti dettati dagli artt. 2 e 3 St. lav., la versione originaria del primo comma dell'art. 4 St. lav. ha designato un destino diverso per il controllo tecnologico, sancendo un divieto assoluto di controllo intenzionale.

La norma infatti vietava in ogni caso, solennemente, al datore di lavoro di effettuare controlli sui propri dipendenti, o meglio sulla loro attività, per mezzo di apparecchiature che lo permettessero a distanza. In tal modo, la disposizione sanciva un limite invalicabile riguardante tanto i mezzi,

---

<sup>62</sup> DE LUCA TAMAJO R., *Presentazione della ricerca*, in DE LUCA TAMAJO R. - IMPERIALI R. - D'AFFLITTO R. - PISANI C. - ROMEI R. (a cura di), *Nuove tecnologie e tutela della riservatezza del lavoratore*, Milano, 1988.

<sup>63</sup> TESTA D.M. – PICCARI M. (con la collaborazione di), “Grande fratello” in azienda con la legge 183/2014 (c.d. *Jobs act*) : profili di riflessione, su [www.iurisprudentes.it](http://www.iurisprudentes.it).

ovverosia gli impianti e tutte quelle altre apparecchiature idonee a consentire un controllo privo di immediatezza a livello spazio-temporale, quanto le finalità, disciplinando contemporaneamente un aspetto molto importante all'interno dei rapporti aziendali.

L'azienda è il luogo in cui la personalità del lavoratore si esprime non solo tramite l'attività lavorativa, ma anche tramite i rapporti che instaura con i propri colleghi. È quindi un suo interesse non essere oggetto di un controllo continuo e meccanico. È inoltre significativo che la disposizione in esame, all'interno della disciplina statutaria, sia inserita nel titolo I dedicato alla libertà e dignità del lavoratore; ciò prova come il bene principalmente protetto dall'art. 4 St. lav. sia la dignità del lavoratore, intesa come diritto di quest'ultimo a svolgere la prestazione in un luogo sereno e non stressante, scevro da condizionamenti che potrebbero derivare da una qualunque forma di controllo occulto e costante.

*“Mentre il controllo umano è contestuale e difficilmente può essere continuativo, il controllo a distanza si attua attraverso un monitoraggio pervasivo occulto e continuativo, che priva il lavoratore di qualsiasi margine di libertà. Si parla di sindrome da pesce rosso, per rappresentare lo stato del soggetto osservato, sottoposto alla spietata osservazione, dell'occhio meccanico, che non dà tregua e non consente alcun riparo”*<sup>64</sup>. E tale osservazione acquisisce un peso maggiore se si considera che, come ha affermato la dottrina più autorevole, l'impresa già di per sé non potrà mai essere democratica, è un'organizzazione di tipo gerarchico, una struttura di potere nella quale il lavoratore, fermo il suo diritto alla controprestazione della retribuzione, ha il dovere di collaborare in forza dell'effetto giuridico tipico connesso alla sottoscrizione del contratto di lavoro. E se in tale contesto subisce anche un pressante e perpetuo controllo, a maggior ragione se occulto, non potrà che assistere alla compressione, se non addirittura al decesso, della sua libertà e dignità individuale, in considerazione della supremazia riconosciuta all'imprenditore, definito capo dell'impresa dall'art. 2086 c.c.<sup>65</sup>

Altra precisazione da fare a proposito del dettato di questo primo comma verte sulla parola “*distanza*”.

Innanzitutto, la prima conseguenza del vietare esplicitamente il controllo a distanza è che risulta decretata la legittimità del controllo esercitato in presenza. Quest'ultimo, a differenza del primo, per sua natura, non è occulto né infinito per la sua attuazione, essendo compreso in un certo lasso

---

<sup>64</sup> IMPERIALI R. – IMPERIALI R., *Controlli sul lavoratore e tecnologie*, Milano, 2012.

<sup>65</sup> Cfr. RIZZI R. – VENTURA A., *La tutela della privacy del lavoratore controllato a distanza*, Consiglio e La Fondazione Nazionale dei Dottori Commercialisti, p. 14; BARBIERI M., *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in TULLINI P., (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017.

temporale<sup>66</sup>. Al tempo stesso, questo non significa che sia sempre legittimo. Non lo è, nel caso in cui dovesse acquisire il carattere della continuità: anche se il lavoratore è sorvegliato a vista dal datore di lavoro, anche se il controllo è effettuato direttamente, di persona, e non è dunque compiuto a distanza, né strumentale, apparendo lecito, l'esercizio del potere di controllo, se continuo, è comunque lesivo della dignità del lavoratore, quindi illegittimo, in quanto diventa vessatorio e asfissiante. Si materializza un contrasto con la regola di carattere generale che impone un ambiente di lavoro amichevole e non stressante.

In secondo luogo, a livello terminologico, il concetto di distanza può essere letto in due diverse accezioni, quella temporale e quella spaziale. Questa importante sfumatura si coglie nella definizione di controlli "a distanza" dell'attività lavorativa, descritti come controlli rientranti nel generale potere di vigilanza del datore di lavoro ed esercitati dal datore stesso mediante l'uso di strumenti in "*posizioni geograficamente diverse ed in periodi successivi rispetto al tempo ed al luogo in cui viene eseguita la prestazione lavorativa*"<sup>67</sup>.

Ricadevano, quindi, nel perimetro della disposizione tutti quei congegni o apparecchiature che potevano registrare e memorizzare dati attingibili dal datore di lavoro in uno spazio e in un luogo diverso da quello in cui il lavoratore veniva controllato.

Gli impianti audiovisivi e le altre apparecchiature tecnologiche sono in grado di registrare tutte le informazioni circa lo svolgimento della prestazione, e dunque inerenti alla persona coinvolta nell'esecuzione, permettendo al datore di lavoro di accantonare tali dati e svolgere in un secondo momento il controllo, che dunque avverrebbe a una distanza temporale. Certo è che in questo caso, se il datore di lavoro venisse a conoscenza di un inadempimento a seguito della verifica delle informazioni immagazzinate si andrebbe a scontrare con il principio di immediatezza della contestazione. L'attributo spaziale è invece riconosciuto alla distanza perché gli strumenti tecnologici, cui fa riferimento l'art. 4 St. lav., consentono al datore di lavoro di sorvegliare il dipendente da un luogo diverso da quello in cui quest'ultimo si trova, creando un'illusione di libertà: il lavoratore non ha in questo caso la possibilità di vedere il suo controllore, subendo un controllo di tipo occulto.

---

<sup>66</sup> In particolare, il controllo umano è un controllo che, oltre a essere temporalmente limitato, si svolge in presenza del soggetto sorvegliato per via del fatto che un uomo ne può controllare un altro solo grazie alle percezioni sensoriali che impongono una vicinanza fisica rispetto all'oggetto materiale del controllo. Ecco perché il controllo in presenza è normalmente trasparente, palese e non occulto; pertanto, difficilmente esso può essere sconosciuto al lavoratore controllato. Si può trarre da ciò, un principio di carattere generale in base al quale il controllo datoriale quando riguarda l'adempimento della prestazione esige la consapevolezza del lavoratore sorvegliato.

<sup>67</sup> CAPOBIANCO M., *Privacy e controlli a distanza: ultimi approdi normativi e giurisprudenziali*, su [www.salvisjurius.it](http://www.salvisjurius.it).

Per quanto riguarda l'oggetto del controllo datoriale, l'opinione largamente condivisa in dottrina e giurisprudenza era quella di un'interpretazione estensiva dell'espressione "attività dei lavoratori", comprendente sia l'attività di adempimento della prestazione, quella specificatamente diretta all'espletamento delle mansioni, sia la condotta complessivamente tenuta dal lavoratore, e dunque qualunque altra attività che, pur essendo annessa cronologicamente all'adempimento della prestazione, lo oltrepassa, attenendo a un momento da esso svincolato, ovvero sia quella attività esorbitante dal momento tecnico-funzionale della subordinazione, denominata in dottrina "licenza comportamentale", come la condotta posta in essere dal lavoratore in pausa<sup>68</sup>.

È evidente dunque come l'art. 4 St. lav., utilizzando l'espressione "attività dei lavoratori", contenga un concetto più ampio di quello degli artt. 2 e 3 St. lav., che si riferiscono a "l'attività lavorativa"<sup>69</sup>: in seguito a consolidate interpretazioni, si ritiene pacificamente che il divieto di cui all'art. 4 St. lav. abbia un perimetro applicativo più esteso, abbracciando anche le manifestazioni della dimensione personale del dipendente, con l'imposizione di un divieto diretto a limitare i controlli che incidono sulla dignità e libertà del datore di lavoro<sup>70</sup>. L'impiego di un concetto dalle maglie più larghe è la prova della volontà del legislatore di tutelare maggiormente i lavoratori laddove i controlli siano effettuati da persone indirettamente, ossia a distanza, mediante impianti audiovisivi e non solo<sup>71</sup>.

L'assolutezza del divieto di controllo intenzionale, includendo nel suo campo di applicazione i monitoraggi effettuabili mediante strumenti esclusivamente destinati al controllo, come le telecamere a circuito chiuso, per cui effettivamente la norma era stata pensata, ha permesso al legislatore di intervenire dunque sull'utilizzo di apparecchiature innegabilmente esterne alla prestazione lavorativa, del tutto lesive della persona del lavoratore: qui siamo di fronte non a un controllo dell'uomo sull'uomo, ma dello strumento tecnico sull'uomo. Siamo di fronte a una sorta

---

<sup>68</sup> Cfr. LISO, *Computer e controllo dei lavoratori*, Giorn. dir. lav. e rel. ind., 1986, pp. 366 ss., riporta l'esempio delle telecamere poste in sala mensa, oppure davanti al locale della rappresentanza sindacale; CROTONDI F. (a cura di), *Diritto del lavoro e delle relazioni industriali*, Milanofiori Assago (MI), 2017; CARINCI M.T., *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.Lgs. 151/2015): spunti per un dibattito*, in *Labour & Law Issues*, vol. 2, no. 1, 2016; CARINCI M.T., *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017; GHEZZI G., *Computer e controllo dei lavoratori*, in *Giorn. Dir. lav. rel. ind.*, 1986, pagg. 358 ss.

<sup>69</sup> Art. 2, comma 3, St. lav.: "È fatto divieto al datore di lavoro di adibire alla vigilanza sull'attività lavorativa le guardie di cui al primo comma, le quali non possono accedere nei locali dove si svolge tale attività, durante lo svolgimento della stessa, se non eccezionalmente per specifiche e motivate esigenze attinenti ai compiti di cui al primo comma". Art. 3 St. lav.: "I nominativi e le mansioni specifiche del personale addetto alla vigilanza dell'attività lavorativa debbono essere comunicati ai lavoratori interessati". DELL'OLIO M., *Art. 4 St. Lav. ed elaboratori elettronici*, in *Dir. Lav.*, 1986, I, afferma che l'attività dei lavoratori è un concetto più ampio di attività lavorativa; e ancora prima di lui, ROMAGNOLI U., *Art. 4*, in SCIALOJA A.- BRANCA G. (a cura di) *Statuto dei diritti dei Lavoratori*, Roma - Bologna, 1979, dichiarava che l'art. 4 St. lav. riguardasse il controllo "esercitato non già sulla sola attività lavorativa, bensì sull'attività in genere dei lavoratori".

<sup>70</sup> BERNARDO P., *Vigilanza e controllo sull'attività lavorativa*, in CARINCI F., *Diritto del lavoro, Commentario*, Torino, 2007.

<sup>71</sup> GOFFREDO M. T. - MELECA V., *Jobs Act e nuovi controlli a distanza*, in *Diritto & Pratica del Lavoro* n. 31/2016.

di “doppiogiochista”: come anticipato, lo strumento tecnico, quale l’impianto audiovisivo, è in grado di assicurare un monitoraggio incessante e occulto, dato che il lavoratore non vede il controllore capace di registrare ogni movimento fisico del dipendente nell’arco della giornata lavorativa, diventando il controllo, così attuato, disumano<sup>72</sup>. Il controllo strumentale è potenzialmente permanente, pertanto vessatorio, potendo catalogare anche momenti di distrazione e disimpegno, presenti nel lavoro di chiunque e che devono essere tollerati, giacché l’uomo, a differenza delle apparecchiature di cui si discute, è una “macchina imperfetta”. Per questo motivo, sin dalla prima fase di lettura dello Statuto dei lavoratori, si era affermata un’interpretazione estensiva della norma secondo la quale, “*il divieto di controllo a distanza investe ogni forma di controllo continuo o, comunque, di controllo attuabile in qualsiasi momento della direzione aziendale sulla prestazione lavorativa*”<sup>73</sup>. La conseguenza di tale lettura normativa è stata la riconducibilità nel divieto “*di qualsiasi forma di controllo a distanza che sottragga al lavoratore, nello svolgimento delle sue mansioni, ogni margine di spazio o di tempo nel quale egli possa essere ragionevolmente certo di non essere osservato, ascoltato o comunque seguito nei suoi movimenti*”<sup>74</sup>.

### **3.2 I controlli preterintenzionali**

Fermo quanto disposto dall’art. 4, comma 1, St. lav., tuttavia con il secondo comma della stessa norma il Legislatore ha compiuto un passo in avanti, introducendo un divieto cd. flessibile.

Con tale previsione è stata fronteggiata un’altra necessità vivida all’epoca dello Statuto dei lavoratori, ossia quella di arginare la tendenza dei datori di lavoro a utilizzare strumenti tecnologici dai quali poteva derivare solo la mera possibilità di un controllo dell’attività lavorativa. Si trattava di strumenti che, non definibili come strumenti di lavoro, non apparendo il loro impiego funzionale all’espletamento delle mansioni, erano comunque presenti in azienda, perché essenziale la loro installazione al soddisfacimento di alcune esigenze che potevano venire a presentarsi<sup>75</sup>.

L’art. 4, comma 2, St. lav. sanciva dunque la legittimità dei controlli preterintenzionali o indiretti, dichiarando che “*gli impianti e le apparecchiature di controllo che siano richiesti da esigenze*

---

<sup>72</sup> Cfr. LEVI A., *Il controllo informatico sull’attività del lavoratore*, Torino, 2013; ALVINO I., *I nuovi limiti al controllo a distanza dell’attività dei lavoratori nell’intersezione fra le regole dello Statuto dei lavoratori nell’intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in “Labour & Law Issues”, vol. 2, no. 1, 2016.

<sup>73</sup> FRENI A. – GIUGNI G., *Lo Statuto dei lavoratori*, Milano, 1971.

<sup>74</sup> ICHINO P., *Il contratto di lavoro*, Milano, 2003.

<sup>75</sup> Un esempio è lo strumento che, adatto a controllare il funzionamento di un macchinario, permetteva contemporaneamente di assumere informazioni sulla quantità e continuità dell’attività lavorativa, ricostruendola.

*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 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*<sup>76</sup>.

Secondo una parte della dottrina<sup>77</sup>, il controllo preterintenzionale costituiva una deroga al divieto di cui al comma 1: il comma secondo rappresentava, per questi autori, un'ipotesi legale di rimozione del divieto di controllo a distanza e la conseguenza di questa loro interpretazione era che i diritti di riservatezza e dignità dei lavoratori potevano essere sacrificati per far fronte alle obiettive necessità organizzative, produttive e di sicurezza dell'impresa. Questa opzione dottrinale, però, portava a ritenere la norma incostituzionale per contrasto con l'art. 41, comma 2, Cost., in quanto implicitamente, ammetteva che il diritto alla dignità e alla riservatezza del lavoratore fosse subvalente nella gerarchia valoriale della Costituzione rispetto alle ragioni produttive e organizzative dell'impresa. L'interpretazione quasi unanime degli interpreti, di conseguenza, aveva guardato al contenuto del secondo comma dell'art. 4 St. lav., non come a una deroga, ma come ribadente un importante principio, quello per cui in nessun caso l'adempimento della prestazione, o più in generale, la condotta del lavoratore potesse essere oggetto di un diretto e voluto controllo effettuato a distanza dal datore.

I controlli preterintenzionali inoltre erano ammessi nel rispetto di due limiti, che ci si accinge a esaminare.

In primo luogo, gli strumenti non dovevano essere direttamente volti a vigilare sul prestatore di lavoro, ma dovevano essere funzionalizzati al soddisfacimento di necessità diverse, tassativamente indicate dalla norma: il controllo preterintenzionale è dunque quel controllo diretto a soddisfare esigenze oggettive differenti dalla mera sorveglianza dei lavoratori, individuando l'aggettivo "*preterintenzionale*" l'elemento psicologico del controllo, ossia la finalità dello stesso<sup>78</sup>. In questi casi, pertanto, il controllo dell'attività lavorativa potrebbe avvenire *praeter intentionem*,

---

<sup>76</sup> La direzione generale del Ministero del lavoro fornisce agli ispettori del lavoro delle indicazioni da rispettare per il rilascio delle autorizzazioni ai sensi dell'art. 4 St. lav., in cui si legge che il relativo provvedimento debba menzionare esplicitamente che 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.

<sup>77</sup> CATAUDELLA A., *Art. 4*, in PROSPERETTI U., *Commentario dello Statuto dei lavoratori*, Milano, 1975; STENICO E., *La tutela della riservatezza del lavoratore nell'esercizio della prestazione*, in *Quad. dir. lav. e rel. ind.*, 2000, n. 24, p. 169.

<sup>78</sup> ROMAGNOLI U., *Sub art. 4* in GHEZZI G. – MANCINI G.F. – MONTUSCHI L. – ROMAGNOLI U., *Statuto dei diritti dei lavoratori*, Bologna, 1972; RUSSO E., *Statuto dei lavoratori: nozioni, limiti e possibilità di deroghe*, in *QFMB Saggi*, 2013 n° 2.

indirettamente e accidentalmente, attesa la potenzialità della strumentazione di controllo impiegata per verificare lo svolgimento della prestazione lavorativa<sup>79</sup>. E ciò lo rende legittimo.

In secondo luogo, infatti, in presenza di tali tassative necessità, ovverosia esigenze organizzative, produttive e di sicurezza del lavoro, per l'installazione degli impianti era richiesto il raggiungimento di un accordo con le organizzazioni sindacali o, in caso di mancato accordo, l'ottenimento dell'autorizzazione amministrativa mediante istanza all'Ispettorato del lavoro<sup>80</sup>. La *ratio* della previsione di una garanzia procedurale a vari livelli si ritrovava nella necessità di contemperare *“l'esigenza di tutela del diritto dei lavoratori a non essere controllati a distanza e quello del datore di lavoro o, se si vuole, della stessa collettività, relativamente alla organizzazione, produzione e sicurezza del lavoro, individuando una precisa procedura esecutiva e gli stessi soggetti ad essa partecipi”*<sup>81</sup>.

Non si può a questo punto sorvolare sul parallelismo con la disciplina dettata dalla l. 604/1966 sul licenziamento. L'art. 3 di tale legge, subordinando il licenziamento individuale a *“ragioni inerenti all'attività produttiva, all'organizzazione del lavoro e al regolare funzionamento di essa”*, limita l'esercizio dei poteri datoriali a esigenze simili a quelle menzionate dall'art. 4, comma 2, St. lav. Prendendo in prestito una nozione tipica del tema dei licenziamenti, l'esercizio del potere di un legittimo controllo a distanza è subordinato alla sussistenza di un *“giustificato motivo oggettivo”*, inteso dalla dottrina maggioritaria come il *“presupposto di fatto dell'atto”*. Si tratta di un limite esterno al potere datoriale, posto a tutela dell'interesse organizzativo del datore e di riservatezza del lavoratore<sup>82</sup>.

Tra l'altro la ricerca dell'equilibrio tra questi due interessi è insito anche nel codice civile. Gli artt. 2104, comma 2, e 2086 c.c. autorizzano il datore di lavoro a monitorare l'attività lavorativa per verificare che il suo svolgimento sia rispettoso delle direttive impartite, come conseguenza necessaria della libertà d'iniziativa economica di cui all'art. 41, comma 1, Cost. Allo stesso tempo il datore è tenuto ad adottare nell'esercizio del suo potere *“le misure necessarie a garantire l'integrità fisica e la personalità morale dei prestatori di lavoro”*, nell'osservanza

---

<sup>79</sup> TUFO M., *I nuovi controlli a distanza tra tecnologie informatiche e privacy del lavoratore*, in BASENGHI F. – RUSSO A., *Flessibilità, sicurezza e occupazione alla prova del Jobs Act*, Torino, 2016; LAMBERTUCCI P., *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli “a distanza” tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs Act)*, in WP CSDLE “Massimo D'Antona” IT, 255/2015.

<sup>80</sup> Cfr. SALIMBENI M.T., *Sub art. 4*, in DE TAMAJO - MAZZOTTA O., *Commentario breve alle leggi sul lavoro*, Padova, 2013; PADOVANI T., *Il controllo a distanza dell'attività lavorativa svolta mediante elaboratori elettronici*, in Riv. It. Dir. Lav., 1985, II, p.252.

<sup>81</sup> Cass., 17 luglio 2007, n. 15982, in Riv. It. Dir. Lav., 2008, n. 3, II, 714 ss., con nota di VALLAURI M.L.

<sup>82</sup> Cfr. NAPOLI M., *La stabilità reale del rapporto di lavoro*, Milano, 1982; PERULLI A., *Il controllo giudiziale dei poteri dell'imprenditore tra evoluzione legislativa e diritto vivente*, in Riv. it. dir. lav., 2015, n.1, I, pp. 83 ss.; ZOLI C., *I licenziamenti per ragioni organizzative: unicità della causale e sindacato giudiziale*, Arg. dir. lav., n.1, I, 2008, pp.31 ss.

dell'art. 2087 c.c. Emerge in quest'ultimo caso l'esigenza di garantire anche la sicurezza del lavoro, richiamata dall'art. 4, comma 2, St. lav. Esigenza che, a differenza di quella organizzativa e produttiva legate strettamente all'interesse datoriale, ha una portata maggiore in quanto è sia, in via diretta, riconducibile alla figura del lavoratore, cioè alla necessità che sia preservata la sua integrità psico – fisica, sia in via indiretta connessa all'opportunità del datore di evitare responsabilità per infortuni sul luogo di lavoro del proprio dipendente, senza dimenticare il terzo frequentatore degli spazi dell'impresa<sup>83</sup>.

In una delle prime pronunce del giudice di legittimità sulla liceità dei controlli preterintenzionali si legge che *“le norme di cui agli artt. 2,3,4, l. 20 maggio 1970 n. 300 tendono a eliminare i sistemi di vigilanza e di controllo che, pur tenendo conto delle esigenze produttive, non sono compatibili con i principi costituzionali così come enunciati in specie dall'art. 41 Cost.; ne consegue che la sorveglianza sui lavoratori non deve avere carattere poliziesco e non può essere realizzata in forme di controllo occulto o a distanza nei confronti dei lavoratori; tuttavia devono considerarsi pienamente legittimi i controlli effettuati sull'attività lavorativa del lavoratore dipendente, il quale nel lavoro da compiere è tenuto all'adempimento di quanto disposto dall'art. 2104 c.c. nell'ambito della collaborazione caratterizzante il rapporto di lavoro subordinato(...)”*<sup>84</sup>.

Un altro caso di asserzione di legittimità dei controlli preterintenzionali è quello dell'Associazione Italiana Allevatori, deputata a eseguire i controlli e le verifiche sull'attitudine produttiva delle aziende zootecniche. Essa aveva presentato al Garante per la protezione dei dati personali, ai sensi dell'art. 17 del d.lgs. n. 196/2003, la richiesta di verifica preliminare relativa al trattamento di dati personali dei propri dipendenti, connesso all'utilizzo di un sistema di localizzazione satellitare basato prevalentemente su tecnologia GPS (global positioning system), per *“organizzare le attività ispettive di propria competenza e di certificare, anche a vantaggio delle proprie strutture periferiche, l'effettività degli accertamenti espletati dal proprio personale presso le aziende di allevamento associate”*<sup>85</sup>.

Si premurava di portare all'attenzione del Garante che al lavoratore sarebbero state garantite riservatezza e libertà di movimento, data la possibilità del dipendente di disattivare il sistema gps in qualunque momento, che sia un momento di non servizio o un momento in cui è obbligato a sospendere l'attività; ferma restando la capacità dell'associazione di identificare l'utilizzatore, incrociando i dati della localizzazione del sistema, della data, dell'ora e del codice seriale

---

<sup>83</sup> LEVI A., (a cura di) *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei lavoratori dopo il Jobs Act*, Milano, 2016.

<sup>84</sup> Cass., 8 ottobre 1985, n.8687 (ud. 28 maggio 1985), in *Mass. Giur. Lav.*, 1986, p.404, con nota di PAPALEONI M.

<sup>85</sup> Garante per la protezione dei dati personali, *Trattamento di dati personali del dipendente mediante sistemi di localizzazione satellitare – 18 febbraio 2010*.

identificativo del dispositivo. I dati acquisiti confluivano in un database gestito dal fornitore dello stesso servizio, erano fruibili all'associazione *“attraverso un portale al quale si accede esclusivamente attraverso l'utilizzo di un sistema identificativo (user id e password)”*, erano accessibili esclusivamente al responsabile del Servizio Personale, al responsabile dei Servizi Ispettivi e al Direttore Generale dell'associazione e infine era assicurata dalla richiedente la loro inutilizzabilità per fini di controllo dell'attività dei lavoratori, e in generale per fini differenti da quelli menzionati.

Nell'accogliere la richiesta dell'associazione di allevatori, ritenendo sussistenti le esigenze di cui all'art. 4, comma 2, St. lav., testo non emendato, il Garante affermava che *“ deve ritenersi che il trattamento di dati personali di localizzazione che l'associazione intende effettuare, in quanto preordinato ad assicurare la corretta ed effettiva organizzazione dell'attività ispettiva alla stessa demandata, non sia illecito. Sebbene, infatti, tali dati siano ricavati mediante l'impiego di "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", non può escludersi che il controllo posto in essere sia giustificato da esigenze organizzative e produttive dell'associazione (art. 4, comma 2, l. n. 300/1970); tale può essere ritenuta, anche in ragione delle sovvenzioni pubbliche ricevute, l'esigenza di documentare, per finalità di rendicontazione dell'associazione, l'effettività delle attività di controllo espletate. Pertanto, ove concretamente osservate le prescrizioni di cui all'art. 4, comma 2 della l. n. 300/1970, l'associazione potrà lecitamente trattare i dati di localizzazione del proprio personale per la finalità dichiarata ”*<sup>86</sup>.

Con la prevista differenziazione dei controlli intenzionali e preterintenzionali, il legislatore ha cercato di garantire da parte dell'art. 4 St. lav. l'assolvimento dello scopo primario per cui era stato formulato: il contemperamento dell'esercizio del potere datoriale di controllo sul corretto adempimento dell'attività lavorativa con la protezione della libertà e dignità dei lavoratori, ritenendo sempre necessario un attento e concreto esame delle peculiarità del singolo caso e garantendo *“una vigilanza sul lavoro ancorché necessaria nell'organizzazione produttiva, in una dimensione umana, e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro”*<sup>87</sup>.

Tuttavia la disposizione in esame presentava un duplice punto debole: il primo era annidato nel fatto che si limitava a dettare le condizioni per l'installazione delle apparecchiature elettroniche,

---

<sup>86</sup> Ibidem.

<sup>87</sup> Cfr. Relazione al d.d.l. Statuto dei lavoratori del Ministro Brodolini; Cass., 17 giugno 2000, n. 8250, in Riv. It. Dir. Lav., 2008, n. 3, II, pp. 714 ss., con nota di VALLAURI M.L.; AMBROSINO A. – CASTIGIONE F., *Nuove forme di controllo a distanza dell'attività lavorativa: aspetti sostanziali e processuale della disciplina statutaria*, in Lavoro e Previdenza oggi, 2011.

senza tracciare il perimetro entro il quale il datore di lavoro legittimamente avrebbe potuto valutare i dati registrati dagli strumenti. Perimetrazione nel frattempo diventata indispensabile alla luce dell'avvento del computer, della posta elettronica e della rete internet, dal cui utilizzo i lavoratori non potevano più prescindere nell'espletamento delle mansioni. Ricordando tra l'altro che il Legislatore storico con l'art. 4 St. lav. era intervenuto a regolare una realtà produttiva diversa da quella emergente, realtà in cui gli strumenti da cui poteva derivare una possibilità di controllo dell'attività lavorativa tendenzialmente non erano considerati funzionali all'esecuzione della prestazione, la norma statutaria non operava una netta distinzione tra i due tipi di strumenti, di controllo e di lavoro, concepita solo da un parte della dottrina, rimettendo alle parti o all'Ispettorato del lavoro il compito di definire i limiti dell'esercizio del potere di controllo a distanza dell'attività dei lavoratori<sup>88</sup>: se da un lato, infatti, una parte della dottrina si era fatta portavoce della necessità di sottrarre gli strumenti di lavoro dall'area di applicazione della norma statutaria, escludendo l'indispensabilità di una preventiva autorizzazione per la loro installazione<sup>89</sup>, la giurisprudenza, dall'altro lato, per dare conto della emergente realtà tecnologica, tendeva a ricomprendere tutte le nuove tecnologie, in particolare, nell'art. 4, comma 2, St. lav., per via della loro "plurifunzionalità"<sup>90</sup>, ossia della loro potenziale capacità ad atteggiarsi allo stesso tempo come strumenti di lavoro e di controllo.

La realtà che si delineava era paradossale: il datore di lavoro anche solo per l'installazione di computer o l'uso della posta elettronica, ormai strumenti di effettuazione della prestazione lavorativa, sarebbe dovuto ricorrere alla procedura sindacale o amministrativa<sup>91</sup>, con inevitabili ripercussioni sulla produttività aziendale e un aggravio organizzativo sul datore. Gli strumenti appena menzionati, figli di una realtà tecnologica in costante divenire, sono dotati d'altronde di una caratteristica di cui erano privi quelli contemplati dalla norma: essendo indispensabili per l'esecuzione della mansione, il loro mancato utilizzo avrebbe messo al rischio l'attività produttiva,

---

<sup>88</sup> MARESCA A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.* in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017.

<sup>89</sup> Cfr. ALVINO I., op. cit.; ICHINO P., *Il contratto di lavoro*, Milano, 2003; Pisani C., *Il computer e l'art. 4 dello Statuto dei lavoratori*, in FRANCO ANGELI, *Nuove tecnologie e tutela della riservatezza dei lavoratori*, 1998, p. 43; Gragnoli E., *L'uso della posta elettronica sui luoghi di lavoro e la strategia di protezione elaborata dall'Autorità Garante*, in Tullini P. (a cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali*, in *Trattato di diritto commerciale e diritto pubblico dell'economia*, diretto da GALGANO F., Padova, 2010.

<sup>90</sup> PISANI C., *I controlli a distanza sui lavoratori*, DLRI, 1987, pp. 121 ss.

<sup>91</sup> Cfr. LAMBERTUCCI P., *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs act)*, in Working papers CSDLE "Massimo D'Antona".IT - 255/2015 pp. 5 ss.; LEVI A. *Il nuovo art.4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Milano, 2016, TULLINI P., *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in *Dir. lav. rel. ind.*, 2009, n. 3, I, pp. 323 ss.

avrebbe potuto sacrificare uno dei due interessi in gioco, l'interesse del datore di lavoro a ottenere un risultato, un profitto meritevole di tutela, tanto quanto il suo opposto.

Se è vero che tali strumenti informatici di lavoro, come il computer, da un lato, consentivano il miglioramento della produzione, dell'organizzazione, della sicurezza del lavoro, è altrettanto corrispondente a realtà che, per le caratteristiche in essi incorporate, permettevano al datore di lavoro di controllare anche il complessivo comportamento tenuto dal lavoratore mentre era in attività. Essi consentivano di assumere dati sulla quantità e continuità dell'attività lavorativa e così di controllare a distanza l'attività svolta dal lavoratore, diventando con il passare del tempo, "un'arma a doppio taglio". E allora, l'operazione di bilanciamento tra esigenza datoriale di verifica dell'adempimento della prestazione e diritto alla riservatezza dei dipendenti è divenuta sempre più ostica, ma essenziale<sup>92</sup>.

L'art. 4, comma 2, St. lav. presentava anche un altro tallone d'Achille.

Come evidenziato, uno dei due limiti da rispettare nell'installazione di potenziali strumenti di controllo era rappresentato dal raggiungimento di un accordo con le rappresentanze sindacali aziendali o dall'ottenimento di un'autorizzazione da parte dell'Ispettorato del lavoro. Tuttavia, sotto questo profilo, la prassi ha registrato una sostanziale inerzia delle imprese e dei sindacati: le prime non si dimostravano propense ad avviare trattative per giungere a un accordo, e i sindacati, dal canto loro, non manifestavano malcontento rispetto all'astensione delle imprese, ritenendo che in questo modo si potevano risparmiare quelli che, nella loro ottica, erano negoziati sindacalmente poco accattivanti e di non agevole gestione. Tale inerzia spingeva il datore di lavoro a eludere diffusamente la norma, finendo per utilizzare i dispositivi al di fuori di qualunque procedura sindacale o amministrativa.

L'unico esito, cui tale situazione apparentemente sembrava portare, era un esito negativo per i lavoratori, ossia l'assenza di una loro tutela.

Eppure, se dalla paralisi del meccanismo predisposto dal secondo comma, la collettività dei lavoratori subiva visibilmente un effetto negativo, ossia l'inefficienza della tutela di riservatezza, il singolo lavoratore, reo di un'infrazione disciplinare, otteneva un vantaggio. Nell'ipotesi in cui quest'ultimo si fosse reso responsabile di un inadempimento, magari anche di grave entità, ma tale inadempimento potesse essere provato dal datore di lavoro esclusivamente con i dati frutto di controlli da lui effettuati in modo non conforme all'art. 4 St. lav., il lavoratore sarebbe riuscito a sottrarsi alla sanzione dovutagli. La giurisprudenza consolidata, infatti, nel silenzio della normativa statutaria, aveva sancito l'inutilizzabilità dei dati raccolti in violazione dell'art. 4, comma 2, St. lav.,

---

<sup>92</sup> ALVINO I., op. cit.

destinando il datore di lavoro all'impossibilità di contestare al lavoratore una sua eventuale condotta inadempiente, nel caso in cui tale contestazione si fosse basata su informazioni, ottenute dal datore stesso, tramite controlli indiretti espliciti in violazione dell'art. 4, comma 2, St. lav., ossia tramite controlli effettuati in assenza di quelle oggettive finalità che fungono da cause giustificatrici o senza il positivo esperimento della procedura richiesta. Una volta installati impianti di sorveglianza *ex art. 4, comma secondo, St. lav.*, le rilevazioni effettuate avrebbero potuto essere utilizzate dal datore di lavoro solo in coerenza con le finalità che ne avevano motivato l'installazione e mai a fini diversi: le stesse autorizzazioni sindacali o amministrative, nel consentire l'impianto delle apparecchiature di controllo, si premuravano di specificare l'inutilizzabilità a fini disciplinari, ad es., delle informazioni memorizzate, in quanto raccolte per specifici scopi<sup>93</sup>.

In questo senso l'art. 4 era sfruttato dal singolo lavoratore "*come scudo individuale per contrastare le iniziative disciplinari del datore di lavoro*"<sup>94</sup>.

### **3.3 I controlli difensivi**

Se la norma statutaria sbarrava decisa la strada all'osservazione dello svolgimento dell'attività lavorativa, non si poteva affermare lo stesso a proposito dei comportamenti illeciti adottati dai dipendenti.

La disposizione presentava una lacuna a tal proposito, astenendosi dal regolare in modo specifico l'ipotesi del controllo a distanza su fatti illeciti dei prestatori di lavoro. E tale lacuna era fonte di rilevanti criticità. Inibire al datore di lavoro l'osservazione mediante controllo meccanico-tecnologico della condotta inadempiente alle obbligazioni lavorative significava impedirgli qualsiasi accertamento e conseguente utilizzo delle prove della condotta tenuta dal dipendente, sul luogo e in orario di lavoro, anche quando questa fosse illecita. A complicare ulteriormente la situazione, la circostanza che la medesima condotta tenuta dallo stesso lavoratore, talvolta, era qualificabile giuridicamente sia come illecito extracontrattuale, o reato per l'ordinamento penale, sia come inadempimento contrattuale. Non si trattava, dunque, solo dell'interesse del datore di lavoro di prevenire ed evitare la tenuta di condotte penalmente rilevanti da parte dei suoi dipendenti, ma anche quello di prevenire illeciti che, pur non essendo di natura penale, erano lesivi per l'azienda, come poteva essere la violazione della privacy aziendale.

---

<sup>93</sup> Cfr. MARESCA A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in TULLINI P., (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017; ALVINO I., *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*, vol.2, no.1, 2016.

<sup>94</sup> MARESCA A., *op. cit.*

L'art. 4 St. lav. si è dimostrato rigido, oltre ogni misura, nel delimitare il potere di controllo datoriale, soprattutto davanti alle accresciute esigenze di difesa del patrimonio aziendale. Anzi, sotto questo profilo, la norma non menzionava né la tutela del patrimonio aziendale, né la prevenzione degli illeciti, tra le finalità del controllo a distanza la cui sussistenza rappresentava il via libera per l'installazione di un'apparecchiatura nel rispetto della procedura di autorizzazione sindacale o amministrativa.

L'esistenza di tale vuoto normativo, aggiunta sia alla circostanza che nuove possibilità di controllo, dischiuse dai moderni strumenti tecnologici<sup>95</sup>, cominciavano a vedere la luce, sia all'assenza di regole sui limiti al controllo dell'impiego di tali strumenti da parte dei lavoratori, è tra le ragioni principali dell'elaborazione della categoria dei "*controlli difensivi*", categoria plasmata dalla giurisprudenza al fine di conciliare l'esigenza di monitoraggio dell'uso degli strumenti tecnologici aziendali da parte del lavoratore con la tutela della dignità e riservatezza di quest'ultimo<sup>96</sup>.

La configurazione dei controlli a distanza a tutela del patrimonio aziendale però più che identificare una creazione giurisprudenziale *ex novo* costituisce un'estensione di orientamenti consolidati all'interno della giurisprudenza formatasi sull'applicazione degli artt. 2 e 3 St. lav., concernenti i controlli umani, o meglio l'impiego da parte del datore di lavoro, rispettivamente, di guardie giurate e del personale di vigilanza, e che sembra opportuno richiamare.

L'art. 2 St. lav. vieta alle guardie giurate di sorvegliare i lavoratori nello svolgimento dell'attività lavorativa e di fare ingresso nei luoghi di lavoro, dove risulti in corso l'esecuzione della prestazione a cui sono addetti i lavoratori<sup>97</sup>, salvo che vi sia una ragione eccezionale legata alla necessità di tutela del patrimonio aziendale (comma 3), tutela rientrante nei compiti delle guardie stesse<sup>98</sup> (comma 1).

L'eccezione sopra menzionata deve inoltre correlarsi "*a esigenze specifiche e motivate, tali da prospettare un pericolo imminente e concreto per il patrimonio stesso, quale l'urgenza di intervenire senza poter attendere l'arrivo della polizia, come in caso di rissa tra dipendenti che*

---

<sup>95</sup> Come visto poc'anzi, posta elettronica, computer e rete internet sono strumenti il cui utilizzo negli anni è diventato imprescindibile per rendere la prestazione lavorativa, per cui condizionarne indistintamente l'utilizzo, e *ab origine* l'installazione, a una preventiva autorizzazione sindacale o ministeriale avrebbe potuto concretare un ostacolo al compimento dell'attività lavorativa.

<sup>96</sup> Cfr. INGRAO A., *Il controllo a distanza realizzato mediante Social network*, in *Labour & Law Issues*, 2016, vol.2, no. 1, p.110; LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Milano, 2016.

<sup>97</sup> Il divieto di accesso nei luoghi di lavoro, proprio perché limitato al lasso temporale necessario a espletare l'attività lavorativa, assolve a una funzione preventiva, in quanto mira a evitare che le guardie giurate possano essere poste in condizione di svolgere di fatto un controllo dell'attività lavorativa dei dipendenti.

<sup>98</sup> Il mancato rispetto di tale disposizione comporta la sospensione della guardia giurata dal servizio e l'irrogazione di una sanzione penale in capo al datore di lavoro inadempiente, ai sensi dell'art. 38 St. lav. Inoltre la violazione del divieto di cui all'art. 2, comma 3, St. lav. implica l'impossibilità per il datore di lavoro di sfruttare quanto segnalato dal personale di vigilanza per provocare l'irrogazione di sanzioni disciplinari.

*metta a repentaglio i beni aziendali o di fuga nei locali di lavoro di un estraneo*<sup>99</sup>. I divieti menzionati al terzo comma evitano l'attuarsi di un controllo intimidatorio, cui potrebbero realizzare le guardie giurate, sia per il timore reverenziale suscitato dalla loro particolare qualificazione giuridica o anche solo per il fatto di essere legittimate a portare con sé un'arma, sia in relazione al regime degli atti posti in essere dalle guardie giurate e al loro valore probatorio, tenuto conto che il verbale redatto dalla guardia giurata fa fede in giudizio fino a prova contraria *ex art. 255 r.d. 6 maggio 1940 n. 635*.

Facendo leva su quanto detto, è cristallino come l'art. 2 St. lav. sia posto nelle condizioni di sancire *“un principio di tutela del luogo di lavoro come luogo riservato al processo produttivo e ai lavoratori che vi sono addetti, dove essi hanno un diritto alla tranquillità”*<sup>100</sup>, consacrato anche dall'art. 4 St. lav.

La norma vieta inoltre alle guardie giurate di contestare ai lavoratori fatti diversi da quelli inerenti alla tutela del patrimonio aziendale (comma 2). Patrimonio aziendale che, a livello nozionistico, secondo la dottrina maggioritaria, deve essere inteso come concetto ampio: le guardie giurate possono dunque essere impiegate per la tutela di tutti i beni aziendali materiali e immateriali, sia di proprietà del datore di lavoro che di soggetti diversi dall'imprenditore, sia che il pericolo provenga dai propri lavoratori, sia che derivi da soggetti estranei all'azienda<sup>101</sup>.

La Corte di Cassazione, nella sentenza del 5 luglio 1991 n. 7455, sfruttando la nozione estensiva di patrimonio aziendale, ha dichiarato legittimo l'incarico della guardia giurata di controllare eventuali mancanze del cartellino segnatempo altrui. In tale pronuncia la Suprema Corte ha ricordato come le guardie giurate possano essere impiegate a tutela del patrimonio aziendale ai sensi dell'art. 2, comma 1, St. lav., e in alcun modo alla sorveglianza sull'attività lavorativa, ai sensi dell'art. 2, comma 3, St. lav., con la conseguente inutilizzabilità dei risultati ottenuti compiendo indagini in violazione del divieto menzionato dal suddetto terzo comma.

Precisa però che le indagini delle guardie giurate possono vertere su atti o comportamenti dei lavoratori quando questi costituiscano possibili fonti di responsabilità extracontrattuale nei confronti dei datori di lavoro e che in tal caso, essendo legittime, i loro risultati sono utilizzabili anche a fini di licenziamento. Il datore di lavoro si è visto riconoscere, da tale sentenza, la possibilità di

---

<sup>99</sup> Cfr. PERONE G.C., *Lo Statuto dei Lavoratori*, su [www.shop.wiki.it/editore/utet\\_giuridica](http://www.shop.wiki.it/editore/utet_giuridica); AMOROSO G. – DI CERBO V.– MARESCA A., *Diritto del lavoro. Lo statuto dei lavoratori e la disciplina dei licenziamenti*, Milano, 2017.

<sup>100</sup> ICHINO P., *Il contratto di lavoro*, Milano, 2003.

<sup>101</sup> Cfr. VALLEBONA A., *Commento agli artt. 1, 2 e 8*, in GRANDI M. - PERA G., *Commentario breve allo Statuto dei lavoratori*, Padova, 1985 p. 6; PERA G. (ASSANTI C.), *Commento allo Statuto dei diritti dei lavoratori*, Padova, 1972, p.17; contra BORTONE R., *Sub art. 2* in GIUGNI G. (diretto da), *Lo Statuto dei lavoratori. Commentario*, Milano, 1979, p. 12 che ritiene legittimo il controllo solo in caso di attentato al patrimonio aziendale da parte di estranei al processo produttivo.

utilizzare il fatto, verificato dalle guardie giurate, di due dipendenti che avevano timbrato il cartellino segnatempo di un altro dipendente, in modo tale che quest'ultimo risultasse uscito un'ora dopo quella in cui aveva effettivamente interrotto l'esecuzione della prestazione lavorativa e lasciato i locali aziendali, permettendogli di percepire indebitamente il compenso per lavoro straordinario indebitamente.

Successivamente con la sentenza del 27 novembre 1992 n. 12675, la Corte di Cassazione ha ritenuto che la prescrizione dell' art. 2 St. lav. di impiegare le guardie giurate solo per scopi di tutela del patrimonio aziendale, il divieto di contestare ai lavoratori fatti non attinenti alla predetta tutela e il divieto di accedere ai locali in cui si sta svolgendo l'attività lavorativa non escludano per il datore di lavoro l'uso di fatti storici inerenti a un lavoratore, a fini disciplinari, accertati dalle guardie giurate fuori dei locali di svolgimento dell'attività lavorativa, negando la configurabilità, in un caso del genere, della violazione dell'art. 2 St. lav. e della lesione della riservatezza del lavoratore<sup>102</sup>. Il caso riguardava furti avvenuti in locali non adibiti all'esecuzione della prestazione lavorativa, mensa e spogliatoio. Nel corso dei controlli di tali locali aziendali, le guardie giurate avevano rilevato la presenza di un dipendente durante l'orario di lavoro e tale fatto era stato utilizzato dal datore come causa fondante il licenziamento disciplinare, poiché ravvisava la violazione dell'obbligo di rispetto dell'orario lavorativo. Secondo la Suprema Corte le guardie giurate non potevano serbare silenzio sul fatto accertato, che il datore di lavoro poteva utilizzare per attivare il recesso dal rapporto, costituendo l'azione del lavoratore un'inadempienza contrattuale.

L'art. 3 St. lav. vieta il controllo occulto sullo svolgimento dell'attività lavorativa, disponendo che *“i nominativi e le mansioni specifiche del personale addetto alla vigilanza debbono essere comunicati ai lavoratori interessati”*<sup>103</sup>.

Secondo la giurisprudenza la norma deve essere letta nel senso che vieta quei controlli effettuati sulla prestazione da soggetti non noti ai lavoratori come controllori, ma non è vietato il controllo oggettivamente occulto eseguito da soggetti abilitati al controllo stesso, una volta conosciuti i loro nomi e quindi garantita la pubblicità della vigilanza sull'attività lavorativa. Secondo tale lettura non si dovrebbe desumere dalla norma un generico divieto di controllo occulto da parte di qualsiasi soggetto<sup>104</sup>.

Sul versante opposto si schiera una parte della dottrina, la quale ritiene che tale controllo potrebbe essere legittimo e conforme ai principi di correttezza e buona fede solo qualora fosse l'unico

---

<sup>102</sup> Cass., 27 novembre 1992, n. 12765, in Riv. Giur. lav., 1993, II, con nota di PETRACCI F.

<sup>103</sup> La violazione di tale divieto comporta l'inutilizzabilità del materiale raccolto, oltre che l'inammissibilità della contestazione disciplinare al lavoratore di sue mancanze conosciute dal datore per mezzo di spie o sorveglianti occulti.

<sup>104</sup> Cass., 9 giugno 1990, n. 5599, in Dir. e Prat. Lav., 1990, 1946; tra le più recenti Cass., 9 luglio 2008, n.18821, in Mass. Giur. It., 2008.

controllo effettuabile per accertare comportamenti illeciti dei lavoratori, non potendosi ignorare la volontà del legislatore del 1970 di vietare, con l'art. 3 St. lav., certe tipologie di sorveglianza, come quella occulta, nel valutare le modalità di compimenti di controlli non esplicitamente disciplinati<sup>105</sup>. La giurisprudenza formatasi in materia ha spesso legittimato la categoria dei controlli difensivi. Nella sentenza n. 5629 del 2000 della Corte di Cassazione si legge che *“la prestazione d’opera da parte del lavoratore subordinato a favore di terzi concorrenti costituisce una violazione d’obbligo di fedeltà che, (...) integra il reato di truffa se svolta nell’orario normale, da parte di soggetto che lucra la retribuzione, fingendo di svolgere il lavoro che gli è stato affidato, mentre svolge altre attività. Ne consegue che, ove sorga il giustificato dubbio che un dipendente incaricato di mansioni da espletare al di fuori dei locali dell’azienda in realtà si renda responsabile di un comportamento illecito di tale genere, è giustificato il ricorso alla collaborazione di investigatori privati per verifiche al riguardo, né sono ravvisabili profili di illiceità a norma dell’art. 2, comma 2, della L. 300 del 1970, il quale prevedendo il divieto per il datore di lavoro di adibire le guardie giurate alla vigilanza dell’attività lavorativa e il divieto per queste ultime di accedere ai locali dove tale attività è in corso, nulla dispone riguardo alla verifica dell’attività lavorativa svolta al di fuori dei locali aziendali da parte di soggetti non inseriti nel normale ciclo produttivo”*<sup>106</sup>.

Come affermato anche da precedenti sentenze, l'imprenditore può verificare il corretto svolgimento dell'attività lavorativa per provare mancanze specifiche dei suoi dipendenti già avvenute o in corso<sup>107</sup>, può verificare la messa in atto di condotte illecite esulanti dalla normale attività lavorativa<sup>108</sup>, e può ricorrere alla collaborazione di investigatori privati<sup>109</sup>. Il caso affrontato dalla sentenza appena richiamata vedeva un istituto di credito sottoporre a verifica l'operato di un suo funzionario incaricato di attività promozionale esterna, a causa dei sospetti generati dagli scarsissimi risultati ottenuti. Emerso che non intratteneva i contatti indicati nei rapporti di servizio, pur non compiendo attività a favore di terzi, il funzionario era stato licenziato. La Cassazione confermava la sentenza impugnata, con cui era stata rigettata l'impugnativa del licenziamento: la verifica sullo svolgimento concreto dell'attività era dunque giustificata e l'ipotesi fatta sulla possibilità che il dipendente potesse spendere il tempo passato fuori dalla banca a favore di terzi rivelava soltanto che la scarsa produttività riportata dal dipendente aveva fatto sorgere il sospetto che avesse adottato un comportamento non elogiabile. Appariva dunque lecito il ricorso a investigatori privati per controllare come il dipendente impiegasse il tempo fuori dalla banca, sia

---

<sup>105</sup> BELLAVISTA A., *Il controllo sui lavoratori*, Torino, 1995.

<sup>106</sup> Cass., 5 maggio 2000, n. 5629.

<sup>107</sup> Cass., 18 febbraio 1997, n. 1455, in Giust. civ., 1997, I, 1261.

<sup>108</sup> Cass., 9 giugno 1989, n. 2813, in Notiz. Giur. Lav., 1989, 289.

<sup>109</sup> Cass., 17 ottobre 1998, n. 10313, su <http://dirittolavoro.altervista.org/>.

perché non rientrante nel raggio di azione del divieto dell'art. 2 St. lav, sia perché diretto a valutare comportamenti che hanno in sé la potenzialità di integrare il delitto di truffa: ove sorga il giustificato dubbio che un dipendente incaricato di mansioni da espletare al di fuori dei locali dell'azienda in realtà tenga un comportamento illecito, è giustificato il ricorso alla collaborazione di investigatori privati per verifiche al riguardo, né sono ravvisabili profili di illiceità a norma dell'art. 2, comma 2, della l. n. 300 del 1970, il quale, prevedendo il divieto per il datore di lavoro di adibire le guardie particolari giurate alla vigilanza dell'attività lavorativa e il divieto per queste ultime di accedere nei locali dove tale attività è in corso, nulla dispone riguardo alla verifica dell'attività lavorativa svolta al di fuori dei locali aziendali da parte di soggetti non inseriti nel normale ciclo produttivo, come ricordato.

Una prima pronuncia della Suprema Corte nell'ambito dell'art. 4 St. lav. risale invece al 3 luglio 2001. In essa, pur non parlando espressamente di “controlli difensivi”, la Corte di Cassazione ha affermato che le norme di cui agli artt. 2 e 3 St. lav., che garantiscono la libertà e la dignità del lavoratore, non escludono il potere dell'imprenditore di controllare, direttamente o mediante la propria organizzazione gerarchica, l'adempimento delle prestazioni lavorative e quindi accertare mancanze specifiche dei dipendenti, indipendentemente dalle modalità del controllo, che può legittimamente avvenire anche occultamente, senza che vi ostino né il principio di correttezza e buona fede, né il divieto di cui all'art. 4 St. lav., riferito esclusivamente all'uso di apparecchiature per il controllo a distanza. Sono pertanto legittimi, in quanto estranei alle previsioni delle suddette norme, gli accertamenti compiuti dall'imprenditore mediante riproduzioni filmate volte a tutelare il proprio patrimonio aziendale, al di fuori dell'orario di lavoro<sup>110</sup>.

Madre putativa della categoria dei controlli difensivi, nell'ambito dell'art. 4 St. lav., è però la sentenza della Corte di Cassazione del 3 aprile 2002 n. 4746.

Con tale pronuncia la giurisprudenza ha affermato l'inapplicabilità dell'art. 4 St. lav. in caso di controlli difensivi, definendo questi ultimi come quei controlli a distanza volti ad accertare condotte illecite dei lavoratori e non l'attività lavorativa<sup>111</sup>: i giudici di legittimità per la prima volta si sono pronunciati in modo esplicito favorevolmente nei confronti dei controlli difensivi statuendo che, riferendosi il divieto di cui all'art. 4, comma 1, St. lav. esclusivamente a controlli che riguardassero l'attività lavorativa, e non emergendo dal secondo comma della disposizione l'esigenza del datore

---

<sup>110</sup> Cass., 3 luglio 2001, n. 8998 su <https://www.avvocato.it/>. In tal senso Cass., 12 agosto 1998, n. 7933, in Notiz. Giur. Lav., 1998, 697.

<sup>111</sup> Nello stesso senso, Cass., 28 gennaio 2011, n. 2117, su <http://www.studiocesarerosso.it/>, ove la Suprema Corte ha ritenuto leciti i controlli difensivi aventi ad oggetto illeciti extra-contrattuali dei dipendenti finalizzati a tutelare il patrimonio aziendale; Cass., 4 aprile 2012, n.5371, su <http://www.avvocatomandico.it/>, ove è confermata la definizione dei controlli difensivi come quelli diretti ad accertare condotte illecite del lavoratore.

di lavoro di tutela del patrimonio aziendale, non vi era ragione di ammettere l'inclusione in tale norma delle forme di controllo diretto ad accertare una condotta illecita.

Il silenzio serbato sul punto dalla disposizione statutaria era perciò tradotto da tale giurisprudenza nella non operatività dell'art. 4 St. lav. per i datori di lavoro che avessero impiegato strumenti tecnologici non per sorvegliare i lavoratori nell'esecuzione della loro prestazione o per perseguire esigenze organizzative o produttive o di sicurezza del lavoro, ma per portare allo scoperto condotte illecite dei dipendenti. Questa non operatività consentiva quindi di ritenere legittimi i controlli difensivi anche nell'ipotesi in cui fossero stati attuati mediante strumenti tecnologici installati senza l'esperimento della procedura richiesta dall'art. 4, comma 2, St. lav. e per un'esigenza diversa da quelle menzionate nella norma<sup>112</sup>.

Nel caso di specie, la sentenza impugnata dal datore di lavoro davanti alla Suprema Corte era una pronuncia del Tribunale di Frosinone che, confermando la precedente sentenza pretorile, aveva dichiarato l'illegittimità del licenziamento intimato nei confronti di un suo giovane dipendente rilevando, tra l'altro, che i fatti contestati al lavoratore si erano rivelati inesistenti o di modesto rilievo, che la società aveva fatto un uso distorto dell'iniziativa disciplinare, e che le sanzioni irrogate, compreso il licenziamento, erano da ritenersi sproporzionate rispetto alle infrazioni commesse dal lavoratore.

La Suprema Corte ha accolto la censura compiuta dal ricorrente della sentenza impugnata per violazione e falsa applicazione degli artt. 4 St. lav., 2106 c.c. (in relazione agli artt. 2104 e 2105 c.c.), 1 e 3 della l. 604/1966, nonché per vizio di motivazione, sostenendo che erroneamente il Tribunale avrebbe ritenuto illegittime le contestazioni relative all'uso privato del telefono aziendale, in quanto fondate su dati acquisiti mediante apparecchiature elettroniche di controllo installate in difetto dei presupposti richiesti dall'art. 4 St. lav.

La Cassazione ha ritenuto fondata la censura in quanto, è vero che l'art. 4 St. lav. vieta l'impiego delle apparecchiature elettroniche per il controllo a distanza, ma ciò avviene quando oggetto del controllo sia l'attività lavorativa. Il divieto è invece da escludersi nell'ipotesi in cui oggetto del controllo sia l'accertamento di una condotta illecita del lavoratore, quando cioè si è di fronte a un controllo difensivo. In presenza di quest'ultima casistica, il difetto dei requisiti di cui al secondo comma dell'art. 4 St. lav. non rende illegittimo il controllo.

In tale pronuncia si legge: *“ai fini dell’operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell’attività dei lavoratori (...), è necessario che il controllo riguardi*

---

<sup>112</sup> Cfr. LAI M., *Utilizzo dei social in ambito di lavoro*, in *Diritto e pratica del lavoro* 5/2020 pp. 290 - 291; MARRAZZA M., *I controlli a distanza del lavoratore di natura “difensiva”*, in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino 2017.

*(direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate*"<sup>113</sup>. La Cassazione, con tale sentenza, ha compiuto una distinzione all'interno della categoria dei controlli del datore di lavoro sulla base della finalità che quest'ultimo si prefiggeva di raggiungere. Questa impostazione consentiva di leggere l'art 4 St. lav. come una norma che permetteva di differenziare i controlli datoriali in tre tipologie di controllo: a) controlli sull'attività lavorativa, sempre vietati dal primo comma; b) controlli preterintenzionali ammessi dal secondo comma se richiesti da esigenze organizzative, produttive o dalla sicurezza del lavoro, e previo responso favorevole della procedura autorizzativa ivi dettata; c) controlli difensivi volti ad accertare condotte illecite dei lavoratori, sempre consentiti, non essendo contemplati dalla norma.

In merito ai controlli difensivi non è tuttavia sufficiente arrestarsi alla sentenza del 2002, sia perchè l'evoluzione giurisprudenziale in materia è consistente, sia per l'influenza, da cui non si può prescindere, esercitata dalla dottrina e da una parte della giurisprudenza di merito, che apparivano ben lungi dall'essere dissuase dall'orientamento giurisprudenziale affermatosi nel 2002. Esaminando il cuore delle criticità emerse, la maggior prudenza degli interpreti era dovuta alla scarsa propensione di forgiare un *tertium genus* di controllo, destinato a essere estrapolato dalla normativa statutaria, per una serie di ragioni.

In primis, la dottrina contestava che, pur di estraniare dall'art. 4 St. lav. i controlli difensivi compiuti a tutela del patrimonio aziendale, la nozione di "attività dei lavoratori" era ricondotta alla mera attività di lavoro, provocando un effetto restrittivo in stridente contrasto con il primo comma, il quale ha adottato una formula onnicomprensiva, come precedentemente rammentato. In secondo luogo, era stata denunciata la difficoltà pratica di discernere i controlli difensivi da quelli sull'attività lavorativa. L'attività di controllo anche se posta in essere dal datore di lavoro per accertare condotte illecite dei dipendenti appariva, agli occhi della dottrina, indissolubile dal controllo sulla stessa prestazione lavorativa. La tesi della sottrazione dal campo di applicazione dell'art. 4 St. lav. dei controlli difensivi è stata mutuata da quella che ammette *ex art. 3 St. lav.* i controlli occulti tramite agenzie investigative finalizzati ad accertare condotte penalmente rilevanti

---

<sup>113</sup> Cass., 3 aprile 2002, n. 4746, su <https://www.altalex.com/>. Nella specie la Suprema Corte ha dedotto che, tenuto conto del lavoro svolto dal ricorrente (guardia giurata), il comportamento del datore di lavoro doveva essere inteso come volto a controllare non l'attività svolta dal lavoratore, bensì la condotta illecita del dipendente, che non avrebbe avuto bisogno del telefono.

dei dipendenti durante il servizio<sup>114</sup>. Però, mentre l'incarico affidato a un'agenzia investigativa può essere circoscritto alle sole indagini necessarie ad accertare la condotta illecita del lavoratore ed essere considerato legittimo proprio perché delimitato, viceversa il controllo tecnologico può registrare l'insieme di tutti i dati relativi all'attività lavorativa. Per quanto il controllo difensivo potesse essere sfruttato per appurare condotte illecite del prestatore di lavoro, le azioni da compiere per porlo in essere erano in grado di permettere l'intercettazione di informazioni circa l'attività lavorativa svolta, anche se non in via diretta. I controlli difensivi, pur avendo un fine specifico, diverso dal controllo sull'esecuzione delle prestazioni, indirettamente lo potevano attuare. Eventualità che l'art. 4 della l. n. 300 del 1970 mira appunto a evitare, partendo dall'assunto ai sensi del quale, *“il controllo deve rimanere in una dimensione quanto più umana, poiché un controllo tecnologico, per le sue caratteristiche (soprattutto la distanza e la continuità nel tempo) è idoneo a ledere la dignità e libertà del lavoratore, facendolo vivere in una condizione di stress costante; esso pertanto deve essere limitato esclusivamente al ricorrere dei peculiari e comprovati requisiti sostanziali e procedurali individuati dall'art. 4, comma 2, St. lav”*<sup>115</sup>.

In terzo luogo, per la dottrina l'orientamento giurisprudenziale era reo di serbare una contraddizione di cui non si poteva non tenere conto: per come costruita dai giudici del lavoro la categoria del controllo difensivo *“finiva per legittimare ex ante l'esercizio del potere datoriale di controllo, in vista di condotte solo eventuali, accertabili cioè solo dopo che il controllo sia stato (illecitamente) effettuato”*<sup>116</sup>.

A fronte di queste convinzioni, agli occhi degli oppositori dell'orientamento giurisprudenziale suddetto, sembrava arduo ipotizzare una concreta distinzione tra i due profili e, pertanto, anche con i controlli difensivi non si poteva che ricadere, inevitabilmente, all'interno della disciplina statutaria. Anche la giurisprudenza di merito si è distaccata parzialmente da quanto dichiarato dalla Cassazione nella sentenza del 2002, procedendo a un ridimensionamento della sua portata. Ha infatti accolto la nozione di controllo difensivo, ma sin dall'inizio, lo ha assoggettato alla procedura sindacale – amministrativa, nel caso in cui fosse strumento di assunzione di informazioni sull'attività del lavoratore.

Questo spiega, almeno in parte, anche il percorso seguito dalla stessa giurisprudenza la quale, partita nel 2002 da un orientamento che voleva i controlli difensivi totalmente avulsi dal campo di

---

<sup>114</sup> Tra le più recenti Cass., 4 dicembre 2014, n. 25674, in *Foro it.*, 2015, I, c. 1671.

<sup>115</sup> DELPIANO C., *Controlli difensivi: l'art. 4 Stat. lav. tra vecchio e nuovo testo*, su <http://www.bollettinoadapt.it>.

<sup>116</sup> MAIO V., *Il regime delle autorizzazioni del potere di controllo del datore di lavoro ed i rapporti con l'art. 8 della legge n. 148/2011*, in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino 2017.

applicazione dell'art. 4 St. lav., successivamente ha fatto rientrare questi ultimi nell'alveo dei controlli preterintenzionali (*ex art. 4, comma 2, St. lav.*)<sup>117</sup>.

Un primo freno a quanto disposto dalla sentenza madre dei controlli difensivi, che considerava legittimi tali controlli in ogni caso, a prescindere dal loro grado di invasività, è stato dato dalla sentenza della Corte di Cassazione del 17 luglio 2007 n.15892<sup>118</sup>.

Con tale pronuncia si afferma un nuovo orientamento per cui non sono oggetto della disciplina dei controlli preterintenzionali contenuta nell'art. 4, comma 2, St. lav. solo quei controlli diretti alla tutela di beni estranei al rapporto di lavoro, ossia non volti a verificare l'esatto adempimento delle obbligazioni lavorative.

Nella vicenda esaminata dalla richiamata sentenza, il controllo sul lavoratore licenziato era stato effettuato mediante il badge assegnato al dipendente per l'ingresso nel garage aziendale destinato alle auto dei dipendenti e per l'ingresso negli uffici. Il dispositivo aziendale consentiva sia la rilevazione dell'identità di chi varcava l'ingresso, sia l'orario in cui ciò accadeva. Questo dato, incrociato con quello dell'ingresso negli uffici, permetteva di controllare l'osservanza dell'orario di lavoro da parte dei dipendenti. Un'apparecchiatura dunque predisposta per il vantaggio dei dipendenti, ma utilizzabile anche in funzione di un controllo della loro osservanza dei doveri di diligenza, nel rispetto dell'orario di lavoro e della stessa correttezza dell'esecuzione della prestazione lavorativa.

Il dispositivo installato nel garage, al contrario di quello predisposto all'ingresso degli uffici, non era stato concordato con il sindacato, né autorizzato dall'Ispettorato del lavoro. Nella pronuncia, la Suprema Corte, dopo aver precisato che il controllo sull'orario di lavoro, e cioè sulla quantità di lavoro, risolvendosi in un accertamento circa la quantità di lavoro svolto, si inquadra, per ciò stesso, in una tipologia di accertamento pienamente rientrante nella fattispecie prevista dal secondo comma dell' art. 4. St. lav., afferma che “ (...) *Né l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore. Tale esigenza, che, con tutta evidenza, ha indirizzato il giudice a quo a decidere nel senso censurato con il conforto, peraltro, anche di pronunce di questa Corte (in particolare, Cass. 3 aprile 2002 n. 4746), non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di*

---

<sup>117</sup> LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza*, Milano, 2016

<sup>118</sup> Cass., 17 luglio 2007, n. 15892, in RGL, 2008, II, p.358, con nota di BELLAVISTA A.: il lavoratore aveva presentato ricorso contro la sentenza della Corte di appello di Milano, la quale aveva dichiarato legittimo il licenziamento intimato nei confronti del ricorrente, riformando parzialmente la sentenza emessa in precedenza dal Tribunale di Milano.

*quei controlli diretti ad accertare comportamenti illeciti dei lavoratori quando tali comportamenti riguardino, come nel caso l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso, ove la sorveglianza venga attuata mediante strumenti che presentano quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro".*

In tale ipotesi, come precisato in seguito dalla Cassazione nella sentenza del 23 febbraio 2010 n. 4375, sussiste un controllo preterintenzionale che rientra nella previsione del divieto "flessibile" di cui al secondo comma dell'art. 4 St. lav.

Nel caso di specie, la Suprema Corte evidenziava la necessità che l'installazione della contestata apparecchiatura dovesse essere oggetto di accordo con le R.S.A. o consentita dall'intervento dell'ufficio pubblico, affinché i dipendenti ne potessero avere piena conoscenza e potessero essere stabilite in maniera adeguata misure di tutela della loro dignità e riservatezza: nel caso concreto, è confermato che non è intervenuto alcun accordo.

Alla luce di ciò, poiché sono assoggettati alla disciplina dell'art. 4 St. lav. anche i controlli difensivi rivolti all'accertamento di condotte illecite dei lavoratori, deve ammettersi l'illegittimità, in assenza di accordo con le R.S.A., dell'installazione di un congegno di sicurezza per l'accesso dei dipendenti al garage aziendale, che permetta la rilevazione di informazioni da cui si ricavi l'osservanza dell'orario e la presenza sul luogo di lavoro; ne deriva l'inutilizzabilità dei dati raccolti con tali modalità a fini disciplinari<sup>119</sup>.

Dunque il controllo operato nei confronti del ricorrente, mediante l'incrocio dei dati, rilevati agli ingressi dell'ufficio con quelli registrati alla sbarra di passaggio del garage aziendale, è stato effettuato illegittimamente, con la conseguente inutilizzabilità dei risultati di tale controllo sull'attività del lavoratore come fondamento dell'intimato licenziamento.

I giudici ritenevano che l'interesse del datore di lavoro a preservare il proprio patrimonio aziendale fosse meritevole di tutela e che lo stesso, in quanto non menzionato dall'art. 4 St. lav. nella versione del 1970, potesse trovare soddisfazione con l'impiego di strumenti di controllo, la cui installazione non doveva essere subordinata ai limiti dettati dalla norma statutaria.

Ed ecco che, se in un primo momento, nella loro totalità, i controlli difensivi erano considerati legittimi anche se effettuati in difetto dei requisiti sostanziali e procedurali indicati nell'art. 4 St. lav., perché, pur apparentemente in contrasto con tale disposizione statutaria, trovavano un'ancora di salvataggio proprio nella loro finalità di scongiurare condotte illecite, in un secondo momento per

---

<sup>119</sup> Cass., 17 luglio 2007, n. 15892, in Riv. It. Dir. Lav., 2008, n. 3, II, 714 ss., con nota di VALLAURI M.L.

rientrare nella zona franca dei controlli difensivi e sfuggire alle maglie applicative dell'art. 4 St. lav., non era più sufficiente allegare la semplice natura difensiva del controllo: includendo la norma, a questo punto, anche una parte dei controlli difensivi (quelli diretti sì ad accertare condotte illecite dei lavoratori, ma quando riguardano l'esatto adempimento della prestazione lavorativa), era necessario un *quid pluris*, dato dalla strumentalizzazione del controllo alla tutela di beni estranei al rapporto di lavoro, beni esorbitanti l'adempimento degli obblighi lavorativi<sup>120</sup>.

Si concretizzava così una sorta di scissione della categoria dei controlli difensivi sulla base e, della finalità e, dell'oggetto del controllo.

Il potere datoriale di controllo a distanza doveva ritenersi svincolato “*dalle maglie strette della procedura sindacale codeterminativa*”<sup>121</sup>, tramite la non applicazione dell'art.4 St. lav. conferendo valore all'esigenza del datore di difesa da comportamenti illeciti a tutela del patrimonio aziendale. “*Sembra efficace l'immagine (...) dei controlli preterintenzionali e quelli difensivi, come due insiemi che hanno un'area di sovrapposizione, cosicchè rientrano nell'area dei controlli preterintenzionali (...) anche i controlli difensivi diretti ad accertare comportamenti illeciti dei lavoratori, laddove l'accertamento consenta di acquisire informazioni sull'esatto adempimento delle obbligazioni nascenti dal rapporto di lavoro*”<sup>122</sup>.

Se inizialmente il tema dei controlli difensivi era stato affrontato da una giurisprudenza orientata in prevalenza ai casi di videosorveglianza, coerentemente con una realtà in cui le telecamere erano uno degli strumenti di controllo più temuti, in un secondo momento, complice l'introduzione dei personal computer nel mondo del lavoro e il correlato utilizzo delle tecnologie rese fruibili dagli stessi a un bacino sempre più esteso di lavoratori (come i software di controllo, il monitoraggio degli accessi alla rete Internet e della posta elettronica), nuove casistiche hanno visto la luce.

Una prima sentenza in materia di monitoraggio degli accessi a internet è la sopra accennata sentenza della Cassazione del 23 febbraio 2010 n. 4375.

Il monitoraggio, da parte del datore di lavoro, della navigazione in Internet sottende l'esigenza di impedire che i lavoratori, pur apparentemente occupati a eseguire le proprie mansioni davanti al computer, diventato un vero e proprio strumento di lavoro nella maggior parte dei casi, in realtà

---

<sup>120</sup> Cfr. BARRACO E. – SITZIA A., *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milanofiori Assago (MI), 2016; MARRAZZA M., *I controlli a distanza del lavoratore di natura “difensiva”*, in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino 2017.

<sup>121</sup> INGRAO A., *Il controllo a distanza realizzato mediante Social network*, in *Labour & Law Issues*, 2016, vol. 2, no. 1 p.110.

<sup>122</sup> ALVINO I., *L'art. 4 dello Statuto dei lavoratori alla prova di Internet e della posta elettronica*, in *Dir. rel. ind.*, 2014, n. 4, p. 1015.

navighino in Internet a scopo personale, togliendo tempo all'attività lavorativa ed esponendo l'azienda a costi e rischi.

Tale esigenza, meritevole di tutela, non cela dall'altro lato che il monitoraggio in questione consente al datore di rilevare l'attività lavorativa, a livello di tempistica e di quantità, ponendosi quindi sia un problema di liceità di tale controllo alla luce dell'art. 4 St. lav., sia un rischio di lesione della sfera di riservatezza del prestatore di lavoro. Infatti il monitoraggio degli accessi a Internet potrebbe finire per memorizzare dati sensibili idonei a rivelare convinzioni religiose, politiche, tendenze sessuali<sup>123</sup>.

La sentenza del 2010 concerne il licenziamento di un lavoratore, cui era stato contestato il reiterato accesso al sistema informatico aziendale e alla rete Internet per ragioni non di servizio, in violazione del regolamento aziendale, con cui i dipendenti venivano informati del divieto di accesso e utilizzo a detti sistemi a scopi personali e del diritto che l'azienda si riservava di accedere ai sistemi. Le informazioni poste alla base del licenziamento erano state ottenute tramite un programma di controllo informatico centralizzato cd. "Super Scout", in grado di acquisire automaticamente le navigazioni in rete dei dipendenti autorizzati all'utilizzo del web, registrando inoltre gli ultimi due mesi di accessi ad Internet.

In linea con la sentenza di primo grado<sup>124</sup>, la Corte di Appello di Milano, 30 settembre 2005, riteneva indispensabile la procedura co-determinativa: è necessaria l'applicazione dell'art. 4 St. lav. qualora il datore di lavoro controlli i collegamenti a Internet tramite strumenti informatici centralizzati, come "Super Scout", a cui i lavoratori non possono accedere e che permettono la memorizzazione dei dati per un certo lasso temporale.

Nella motivazione si legge: *"I programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione dell'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento"*.

---

<sup>123</sup> BARRACO E., *Utilizzo delle e-mail ed Internet da parte del dipendente per uso privato*, su [www.csdn.it/images/relazioni/relazione\\_barraco](http://www.csdn.it/images/relazioni/relazione_barraco).

<sup>124</sup> I fatti alla base del licenziamento del lavoratore erano stati acquisiti dal datore di lavoro tramite l'impiego di uno strumento come "Super Scout", che, per il Tribunale, consente al datore stesso di sorvegliare a distanza, senza immediata percezione del controllo da parte del dipendente destinatario, tutte le navigazioni in Internet, la loro durata, la loro frequenza, verificando come ciascuno dei dipendenti impieghi il tempo di collegamento ad Internet, se a fini personali o a fini aziendali. Tali informazioni finiscono per essere estese anche ai tempi e alle modalità di svolgimento dell'attività lavorativa dei dipendenti autorizzati all'uso di Internet. Il controllo effettuato tramite "Super Scout" rientra dunque nell'art. 4, comma 2, St. lav. e, data l'avvenuta installazione del programma senza il previo esperimento della procedura dettata dalla norma, è illegittimo. E i dati raccolti sono inutilizzabili.

Nonostante la loro natura di apparecchiature di controllo a distanza, con tali programmi non si ricade nell'art. 4, comma 1, St. lav., ritenendo meritevole di tutela la necessità di tutelare i sistemi informatici aziendali da aggressioni informatiche esterne. Il loro utilizzo è quindi consentito nel rispetto di quanto disposto dal secondo comma.

Nel punto conclusivo la sentenza della Corte d'Appello arrivava ad affermare che *“in ogni caso anche per i controlli difensivi la legittimità di apparecchiature per il controllo a distanza è comunque condizionata al rispetto della regola procedimentale di cui all'art. 4, comma 2, St. lav.”*. A fronte di ciò, anche in appello è stata ribadita l'inutilizzabilità dei dati raccolti in violazione della richiamata procedura statutaria.

La Suprema Corte, con la nota sentenza del 23 febbraio 2010 n.4375, ha confermato quanto statuito dalla Corte d'Appello in quanto: *“In tema di controllo del lavoratore, le garanzie procedurali imposte dall'art. 4, secondo comma, della legge n. 300 del 1970 per l'installazione di impianti ed apparecchiature di controllo 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, trovano applicazione anche ai controlli c.d. difensivi, ovverosia a quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela dei beni estranei al rapporto stesso, dovendo escludersi che l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti possa assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore”*.

Il monitoraggio della posta elettronica è fonte di problematicità addirittura maggiori rispetto a quelle sottolineate per il controllo degli accessi alla rete Internet.

Con la sentenza della Suprema Corte del 23 febbraio 2012 n.2722 la tematica dei controlli difensivi viene esaminata proprio in riferimento al controllo delle e- mail.

In applicazione dei principi espressi dalle richiamate pronunce del 2007 e del 2010, la Corte nella sentenza in esame, relativa al caso di un lavoratore licenziato perché accusato di aver divulgato a mezzo di messaggi di posta elettronica diretti ad estranei notizie riservate concernenti un cliente dell'Istituto e aver compiuto, grazie a tali informazioni, operazioni finanziarie da cui aveva tratto profitto, ha ritenuto correttamente motivata una sentenza di merito che *“aveva considerato alla stregua delle apparecchiature di controllo vietate (ove non fatte oggetto della procedura di validazione prevista dall'art. 4, e. 2) i programmi informatici che consentono il monitoraggio dei messaggi della posta elettronica aziendale e degli accessi Internet, ove per le loro caratteristiche consentano al datore di controllare a distanza ed in via continuativa durante la prestazione,*

*l'attività lavorativa e il suo contenuto, per verificare se la stessa sia svolta in termini di dirigenza e di corretto adempimento, sotto il profilo del rispetto delle direttive aziendali (Cass. n. 4375 del 2010)".*

Per il Collegio, la fattispecie in esame è estranea al campo di applicazione dell'art. 4 St. lav. poiché il c.d. controllo difensivo messo in pratica dal datore non riguardava l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa immagine dell'Istituto bancario presso i terzi.

Il datore di lavoro ha infatti posto in essere una vigilanza sulle strutture informatiche aziendali *"che prescindeva dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti ed era, invece, diretta ad accertare la perpetrazione di eventuali comportamenti illeciti"*.

In questo caso entrava in gioco il diritto del datore di lavoro a tutelare il proprio patrimonio, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna e *"(...) Tale situazione è già esclusa dal campo di applicazione dell'art. 4 dalla sopra citata giurisprudenza (che già esclude dai controlli difensivi vietati quelli aventi ad oggetto la tutela di beni estranei al rapporto di lavoro, v. Cass. n. 15892 del 2007)"*.

Esula quindi dal campo di applicazione della norma il caso del datore che abbia compiuto verifiche indirizzate ad accertare comportamenti del prestatore di lavoro illeciti e lesivi del patrimonio e dell'immagine aziendale.

In attuazione di tale principio, è stato ritenuto legittimo il controllo effettuato dall'istituto bancario sulla posta elettronica aziendale del lavoratore accusato di aver diffuso notizie riservate concernenti un cliente, e, di aver eseguito operazioni finanziarie per lui redditizie.

E invero non vi è controversia in materia di monitoraggio degli accessi alla rete o, come nel caso attualmente sotto la nostra lente di ingrandimento, della posta elettronica, in cui i datori di lavoro, a fronte della sostenuta illegittimità per violazione dell'art. 4 St. lav. da parte del lavoratore, non facciano leva sulla portata meramente difensiva della sorveglianza, attuata non per controllare l'adempimento della prestazione lavorativa, ma a protezione del patrimonio aziendale, piuttosto che del sistema informatico da probabili aggressioni esterne, per aggiudicarsi l'immunità dalla procedura imposta dal secondo comma della norma stessa e dalle sanzioni conseguenti al mancato rispetto della stessa.

Altro punto da segnalare di tale pronuncia è che è riconosciuta la legittimità dei controlli difensivi effettuati in seguito al sorgere del sospetto nel datore di lavoro di comportamenti illeciti da parte dei propri dipendenti, in presenza di elementi indiziari circa la loro commissione. Precisando che *"il datore ha compiuto il suo accertamento ex post, ovvero dopo l'attuazione del*

*comportamento addossato al dipendente, quando erano emersi elementi di fatto tali da raccomandare l'avvio di un'indagine retrospettiva*", la Suprema Corte ha escluso l'operatività dell'art. 4 St. lav. in ordine a una sorveglianza sulle strutture informatiche aziendali, avendo il datore compiuto l'accertamento *ex post*, dopo l'attuazione della condotta imputata al dipendente, quando erano emersi elementi legittimanti l'avvio di un'indagine retrospettiva<sup>125</sup>.

Questi controlli cd. successivi si contrappongono ai cd. controlli difensivi preventivi. Questi ultimi rispondono alle azioni poste a difesa di legittimi interessi datoriali, attuate in modo preventivo e indiscriminato (non sono conseguenti a un sospetto certificato e mirato) a tutela di beni o del patrimonio aziendale, per verificare la correttezza dei dipendenti nell'esecuzione della prestazione e per prevenire eventuali abusi: tale controllo, quindi, si pone come obiettivo principale, il controllo generale sul rispetto delle regole in misura di prevenzione.

A termine di quanto ora esplicito, è utile aggiungere che oltre alla questione dell'applicabilità o meno dell'art. 4 St. lav. e della disciplina del trattamento dei dati personali, deve tenersi in considerazione la tutela della corrispondenza e della sua segretezza.

A tal proposito si ricorda l'art. 15 Cost. per cui *“ la libertà e la segretezza della corrispondenza sono inviolabili”* e una *“loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge”*.

A sostegno poi della garanzia costituzionale si menziona la sussistenza della normativa penale volta a sanzionare il delitto di violazione, sottrazione e soppressione di corrispondenza<sup>126</sup>.

Infine, un'ultima pronuncia da rammentare a proposito dei controlli difensivi nell'ambito dell'art. 4 St. lav. che, a completamento di questa disamina, si pone in linea con quanto statuito nel 2010, è la sentenza della Suprema Corte del 1 ottobre 2012 n. 16622, relativa al caso di un operatore telefonico di centrale di prima assistenza stradale e automobilistica, licenziato *“per aver intrattenuto, nel periodo 1 agosto - 29 ottobre 2004, n. 460 contatti telefonici inferiori a 15 secondi (tempo non sufficiente per sentire le richieste degli utenti e rispondere) e di aver effettuato 136 telefonate personali”*.

---

<sup>125</sup> LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori*, Milano, 2016

<sup>126</sup> Si tratta degli artt. 616 – 618 c.p. L'art. 616 c.p. in particolare stabilisce che *“chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da trenta euro a cinquecentosedici euro.*

*Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocimento e il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni.*

*Il delitto è punibile a querela della persona offesa.*

*Agli effetti delle disposizioni di questa sezione, per "corrispondenza" s'intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza”.*

Queste informazioni erano state ottenute mediante un sistema di rilevamento delle telefonate attraverso il software Blue's 2002 che, nonostante consentisse un controllo a distanza sull'attività lavorativa e fosse stato installato senza accordo con le O.O.S.S., era stato ritenuto non in contrasto con l'art. 4 St. lav., in quanto relativo al c.d. controllo difensivo, sia dal Tribunale che dalla Corte di Appello di Roma, a cui il lavoratore era ricorso per ottenere rispettivamente la declaratoria di illegittimità del licenziamento e, a fronte del rigetto della domanda, l'annullamento della sentenza del predetto Tribunale.

Con la sentenza del 2012, la Suprema Corte ha cassato la pronuncia della Corte d'Appello, ritenendo che quest'ultima non avesse correttamente applicato i principi di diritto espressi dalla richiamata sentenza della Corte di Cassazione n. 4375 del 2010 e ai quali intendeva dare continuità<sup>127</sup>.

La Cassazione ha affermato inoltre che *“l'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che anche per i c.d. controlli difensivi trovino applicazione le garanzie del citato art. 4, secondo comma, e che, comunque, quest'ultimi, così come la altre fattispecie di controllo ivi previste, non si traducano in forme surrettizie di controllo a distanza dell'attività lavorativa dei lavoratori. Se per l'esigenza di evitare attività illecite o per motivi organizzativi o produttivi, possono essere installati impianti ed apparecchiature di controllo che rilevino dati relativi anche alla attività lavorativa dei lavoratori, la previsione che siano osservate le garanzie procedurali di cui all'art. 4, secondo comma, non consente che attraverso tali strumenti, sia pure adottati in esito alla concertazione con le r.s.a., si possa porre in essere, anche se quale conseguenza mediata, un controllo a distanza dei lavoratori che, giova ribadirlo, è vietato dall'art. 4, comma 1, cit.. Il divieto di controlli a distanza ex art. 4, della legge n. 300 del 1970, implica, dunque, che i controlli difensivi posti in essere con il sistema informatico Blue's 2002, ricadono nell'ambito dell'art. 4, comma 2, della legge n. 300 del 1970, 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”*.

---

<sup>127</sup> Cass., 1 ottobre 2012, n.16622 *“in tema di controllo del lavoratore, le garanzie procedurali imposte dall'art. 4, secondo comma, della legge n. 300 del 1970 per l'installazione di impianti ed apparecchiature di controllo 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, trovano applicazione anche ai controlli c.d. difensivi, ovverosia a quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela dei beni estranei al rapporto stesso (Cass., n. 2722 del 2012, n. 4375 del 2010)”*.

Non viene dunque negata l'esistenza della categoria dei controlli difensivi sottratti al perimetro dell'art. 4 St. lav. dalla Suprema Corte, ma, in linea con la più moderata visione dei giudici di merito<sup>128</sup>, viene ridotta la sua area di applicazione, includendovi solo i controlli diretti ad accertare comportamenti illeciti dei lavoratori idonei a pregiudicare beni estranei al rapporto di lavoro: la possibilità dei controlli difensivi si arresta, dunque, davanti al diritto alla riservatezza del dipendente, al punto che *“l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore”*<sup>129</sup>, non essendo possibile espungere tout court la categoria dei controlli difensivi della fattispecie astratta disegnata nel secondo comma dell'art. 4 St. lav. Tuttavia anche tale orientamento restrittivo è stato bersaglio di critiche, essendo stata riscontrata una difficoltà pratica nel distinguere tra comportamenti lesivi di beni estranei e interni al rapporto di lavoro. A ciò si aggiunga che la dottrina aveva portato in superficie il fatto che era tutt'altro che spianata la strada per giungere a una nozione unanimemente condivisa di "patrimonio aziendale" e a un'identificazione dei beni estranei al rapporto di lavoro, con un'inevitabile discrezionalità valutativa dell'interprete.

A pesare vi era anche la circostanza che, nonostante queste pronunce, i confini della fattispecie dei “controlli difensivi” continuavano a non essere ben delimitati; la giurisprudenza di legittimità, pur avendo “corretto il tiro” rispetto alla sentenza del 2002 mediante l'inclusione dei controlli difensivi relativi al corretto adempimento delle obbligazioni discendenti dal rapporto di lavoro nell'alveo dell'art. 4, comma 2, St. lav., proseguiva a considerarli come un gruppo autonomo.

La situazione era complicata inoltre dalla normativa sulla privacy.

Anche i controlli difensivi estranei all'art. 4 St. lav., in quanto tenuti al rispetto della disciplina generale sulla riservatezza, devono essere realizzati con modalità non eccessivamente invasive e rispettose delle garanzie di libertà e dignità dei dipendenti; è necessario che il datore di lavoro attivi i controlli solo quando questi risultino necessari e/o indispensabili, rendendoli il meno intrusivi possibili. Ecco perché, quando vi è la possibilità, il controllo deve essere eseguito su dati anonimi o aggregati, non direttamente riconducibili ai lavoratori.

---

<sup>128</sup> Come visto già nel 2005 i giudici di merito, in una pronuncia sul monitoraggio degli accessi ad Internet, avevano sostenuto che in ogni caso anche per i c.d. controlli difensivi la legittimità delle apparecchiature per il controllo a distanza è comunque condizionata al rispetto della regola procedimentale di cui all'art 4, comma 2, St. lav. In questo senso App. Milano, 30 settembre 2005, in D&L, 2006, p. 899

<sup>129</sup> Cfr. ALVINO I., *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*, in Labour & Law issues, 2016, vol. 2, no.1, p.14; Cass., 17 luglio 2007, n. 15892, in RGL, 2008, II, P.358, con nota di BELLAVISTA A.; Cass., 23 febbraio 2010, n. 4375, su <https://www.ricercagiuridica.com/>; Cass., 23 febbraio 2012, n. 2722, su <http://www.avvocatomandico.it/>.

A titolo esemplificativo può ricordarsi la sentenza della Corte di Cassazione del 1° agosto 2013 n. 18443<sup>130</sup>, nella quale si afferma che il trattamento di informazioni, indicative degli specifici contenuti degli accessi dei singoli siti web visitati, realizzato dal datore di lavoro senza il consenso del dipendente, si configura come un trattamento di dati eccedente rispetto alle finalità perseguite, dal momento che il datore di lavoro avrebbe potuto dimostrare l'illiceità del comportamento del dipendente, in rapporto al corretto uso degli strumenti affidati sul luogo di lavoro, limitandosi a provare in altro modo l'esistenza di accessi indebiti alla rete e i tempi di collegamento<sup>131</sup>. Inoltre sebbene i dati personali siano stati raccolti nell'ambito di controlli informatici volti a verificare l'esistenza di un comportamento illecito, le informazioni di natura sensibile possono essere trattate dal datore di lavoro senza il consenso quando il trattamento necessario per far valere o difendere un diritto in sede giudiziaria sia indispensabile: tale indispensabilità non ricorre nel caso di specie.

In conclusione, alla luce del quadro giurisprudenziale fin qui rappresentato, sono prospettabili tre situazioni. Nel caso in cui il controllo del datore di lavoro avvenga in forma occulta e non sia cioè rilevabile dal lavoratore, il quale subirà un controllo a distanza avente unicamente come oggetto l'attività lavorativa, il controllo è vietato dal primo comma dell'articolo 4 dello Statuto dei lavoratori; nella differente ipotesi in cui il controllo annoveri, tra i propri fini, quello primario di prevenire e/o proteggere la sicurezza dell'azienda stessa e delle sue informazioni, piuttosto che soddisfare esigenze organizzative e produttive e, soltanto in via secondaria e sussidiaria, quello di consentire la sorveglianza della prestazione lavorativa, il controllo è consentito nel rispetto delle modalità previste dal secondo comma dell'articolo 4 dello Statuto dei lavoratori; infine se l'installazione degli strumenti tecnologici è predisposta per un controllo che non riguardi in alcun modo l'attività lavorativa, ma sia unicamente diretto ad accertare, seppur in modo occulto, eventuali condotte illecite del lavoratore e, in particolare, risulti indispensabile per la tutela del patrimonio aziendale, il controllo non rientra nell'ambito di applicazione dell'art. 4 St. lav. e non richiede per la sua legittimità il previo esperimento della procedura sindacale o amministrativa<sup>132</sup>.

---

<sup>130</sup> Cass., 1° agosto 2013, n. 18443, su <https://www.miolegale.it/>.

<sup>131</sup> La titolare di una casa di cura era ricorsa per Cassazione contro la sentenza del Tribunale di Palermo del 26 giugno 2008 con cui è stato respinto il suo ricorso, presentato ai sensi del d.lgs. n. 196 del 2003, art. 152, contro il provvedimento con il quale il Garante per la protezione dei dati personali le aveva vietato il trattamento dei dati personali di un proprio dipendente, dal cui computer erano stati estratti dati concernenti l'accesso a internet, tali da configurare "dati sensibili" perché relativi a convinzioni religiose e politiche nonché alle tendenze sessuali. Inoltre il Garante aveva ravvisato la mancanza di trasparenza nel comportamento della società che aveva compiuto accertamenti in assenza di una previa informativa all'interessato relativa al trattamento dei dati personali.

<sup>132</sup> FERRARA F. – PAGLIARI F., *Limiti dei controlli difensivi sul lavoratore alla luce delle ultime pronunce della Corte di Cassazione*, su [www.filodiritto.com](http://www.filodiritto.com).

#### **4. Il diritto alla riservatezza: profili introduttivi**

La tutela del lavoratore assoggettato a controlli a distanza viene affidata anche al d.lgs. n. 196/2003, il Codice della privacy. L'art. 4 St. lav., così come scritto nel 1970 e da allora rimasto invariato fino al 2015, è stato rinvigorito nella sua efficacia applicativa dalla disciplina del Codice della privacy che, in merito ai controlli a distanza, ha operato una sorta di duplicazione regolativa, riconfermando l'operatività dell'art. 4 St. lav. anche in riferimento alla disciplina della tutela della riservatezza<sup>133</sup>. In particolare, fino all'intervento del d.lgs. n. 101/2018, di cui si tratterà in seguito, l'art. 114 del d.lgs. n. 196/2003 rinviava esplicitamente allo Statuto, statuendo che, con riguardo ai profili della privacy legati ai controlli a distanza posti in essere dal datore di lavoro, “*resta fermo quanto disposto dall'art. 4 della legge 20 maggio 1970, n. 300*”. Tuttavia è opportuno sottolineare come non sia stato tanto il precetto legale di cui all'art. 114 del d.lgs. 196/2003 a limitare i controlli datoriali a distanza, quanto l'attività del Garante per la protezione dei dati personali, che ha assunto una posizione netta di chiusura: ha ritenuto di far valere il principio di necessità in materia, che impone di prevenire l'abuso degli strumenti aziendali, mediante l'adozione di adeguate misure organizzative e tecnologiche<sup>134</sup>. Il Garante giustifica questo suo atteggiamento rigoroso con la circostanza che il datore, tramite il controllo a distanza, potrebbe venire a conoscenza di dati sensibili del lavoratore. Emerge la doppia anima regolativa della materia dei controlli a distanza, impossibilitata a esaurirsi in quella lavoristica, dovendosi dar voce anche all'altra esigenza che viene in rilievo, consistente nella tutela della riservatezza<sup>135</sup>.

Ai fini della presente analisi, si rende dunque necessaria anche una preliminare ricostruzione della disciplina in materia di privacy, un diritto di assai complessa definizione.

#### **4.1 Le origini del concetto di privacy negli Stati Uniti D'America**

Tradizionalmente le origini moderne della privacy, reso in italiano come riservatezza, si fanno risalire a due giuristi statunitensi, Samuel Warren e Louis Brandeis, che hanno dato alle stampe un saggio intitolato “*The Right to Privacy. The Implicit Made Explicit*”.

L'opera rappresenta una pietra miliare in materia di privacy, giacché è la prima monografia giuridica a riconoscere l'esistenza di un autonomo diritto alla riservatezza.

I due giuristi, originari di Boston, hanno affermato l'esistenza, all'interno dell'ordinamento giuridico americano, di un autonomo diritto definito come “*the right to be let alone*” (diritto di essere lasciato solo/indisturbato).

---

<sup>133</sup> In argomento si veda TROJSI A., *Il diritto del lavoratore alla protezione dei dati personali*, Torino, 2013.

<sup>134</sup> Secondo il Garante, il datore di lavoro che voglia evitare che il proprio dipendente adoperi il computer aziendali per fini personali dovrebbe prediligere un approccio preventivo, evitando a priori che ciò possa accadere.

<sup>135</sup> LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Milano, 2016

Era il 1890 e i due giovani avvocati stavano preparando una causa contro le indiscrezioni sulla vita matrimoniale della moglie dello stesso Warren da parte di quello che era stato uno dei primi giornali a utilizzare la stampa a rotativa, la Evening Gazette di Boston. Guardando alla stampa a rotativa, veloce ed efficiente metodo di diffusione delle notizie, come a un'innovazione tecnologica che aveva il potere di modificare profondamente il loro impatto sulla società, Brandeis e Warren, secondo i quali la vita privata doveva ritenersi come un recinto invalicabile, avevano iniziato a interessarsi a una serie di casi, in cui le invenzioni del tempo, come la fotografia, potevano essere causa di violazioni della riservatezza dell'individuo, divulgando dettagli e particolari sulla vita privata di ognuno. Ne è venuto fuori il saggio, innesco della discussione sul concetto stesso di privacy. I due avvocati si erano ritrovati dunque a riflettere su quali informazioni riguardanti la vita personale di un individuo dovessero essere di pubblico dominio e quali, invece, meritassero una tutela dall'invasione altrui<sup>136</sup>. Loro ritenevano necessario proteggere l'essenza del diritto alla privacy non per il valore che esso ha nel pubblico, ma per il valore che esso possiede per il suo titolare. Una scelta, quindi, quella dei due giuristi, che mette al centro la persona e il suo valore. Dopo la pubblicazione del "The Right to Privacy", negli Stati Uniti l'elaborazione dottrinale in materia di privacy è stata scarsa e ciò ha rafforzato il ruolo dei giudici, i quali hanno chiarito alcuni principi dell'ordinamento giuridico americano riuscendo, attraverso un'interpretazione evolutiva degli emendamenti del Bill of Rights, a rintracciare il fondamento giuridico del diritto alla privacy. L'atteggiamento della giurisprudenza nei confronti dell'esigenza di privacy è stato però altalenante: mentre una parte della società americana e una minoranza dei giudici della Corte Suprema propugnava un approccio difensivo della libertà e, nello specifico, della privacy, l'altra parte della società e la maggioranza dei giudici della Corte Suprema erano ostili verso il riconoscimento di un autonomo diritto alla riservatezza. Tale situazione d'incertezza ha cominciato ad attenuarsi a partire dagli anni sessanta del secolo scorso, quando sono state emesse una serie di sentenze decisive, con le quali la Corte Suprema ha riconosciuto la privacy come oggetto di tutela in rapporto sia alla vita pubblica che privata dell'individuo. Nel 1970, per mettere un punto al dibattito nato e per soddisfare la necessità di un intervento normativo è stata emanata una legge, il cd. *Privacy Act*, che ancora oggi rappresenta un importante testo normativo di riferimento in materia di privacy<sup>137</sup>.

---

<sup>136</sup> IASELLI M. – GORLA S., "Storia della Privacy", Roma, 2015.

<sup>137</sup> Cfr. PAGALLO U., *La tutela della privacy negli Stati Uniti d'America ed in Europa*, Milano, 2008; RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995.

## 4.2 Il diritto di privacy: quadro nazionale e comunitario

Lo sviluppo tecnologico e il connesso avvento della società dell'informazione dell'informatica provocano inevitabilmente continui cambiamenti delle forme organizzative, tecnicizzando il lavoro, e rendono al tempo stesso disponibili strumenti e metodi di raccolta d'informazioni personali avanzati e invasivi, un tempo neanche lontanamente immaginabili. A fronte di tale espansione tecnologica, che innegabilmente consente ai datori di lavoro di incrementare l'efficienza produttiva tramite un'intensa attività di sorveglianza della prestazione dei propri dipendenti, dato l'inserimento dell'individuo nella società "globale", nella quale la stragrande maggioranza delle azioni compiute e delle scelte individuali lasciano una "traccia" che ne consente la mappatura e con essa la ricostruzione dell'identikit della persona, l'individuo stesso ha cominciato a maturare e vantare una vera e propria pretesa al controllo del flusso delle informazioni a lui relative, consapevole che le nuove tecnologie serbano la potenzialità di produrre dati, il cui sfruttamento potrebbe mettere a repentaglio la sua tranquillità, la sua identità a discapito delle relazioni sociali<sup>138</sup>; onde per cui l'esigenza di verificare le conseguenze dell'evoluzione tecnologica sui rapporti umani nei luoghi di lavoro.

Esemplificativo del fenomeno di cui si tratta è un caso risalente agli inizi degli anni sessanta del secolo scorso: un datore di lavoro aveva modificato i gabinetti di decenza della fabbrica, privandone le porte delle serrature e creando all'interno di ogni porta delle aperture rettangolari ad altezza d'uomo, coperte da vetro trasparente attraverso le quali era possibile osservare quanto accadeva in ciascun gabinetto<sup>139</sup>. L'invasività del controllo eseguito è lampante. Nella motivazione dell'ordinanza si legge che l'apertura delle "finestrelle" aveva *"il preciso scopo di creare all'interno della fabbrica un clima oppressivo che valesse a scoraggiare gli operai da iniziative sindacali: il lavoratore che sa di essere controllato dalla direzione perfino nel suo atto più innocuo e normale, qual è il bisogno fisiologico, è verosimilmente portato a ritenere che egualmente egli sarà sotto controllo in ogni altro discorso o atteggiamento specie se di tipo sindacale"*.

L'introduzione degli spioncini alle porte dei gabinetti di decenza è espressione di un apparato di controllo, potenzialmente repressivo, cui è sottomesso l'operaio.

In Italia è stata la giurisprudenza ad avere un ruolo fondamentale nella genesi e nella disciplina del diritto alla riservatezza. La giurisprudenza è intervenuta per porre un freno alle incertezze che stavano dominando a causa del silenzio serbato dal legislatore sulla sussistenza o meno di un diritto

---

<sup>138</sup> CARIGLINO F. - BENVENÙ A. – PARUZZO F., *Diritto dell'Internet*, Padova, 2016.

<sup>139</sup> Pret. Monopoli, ordinanza 27 ottobre 1970, in Foro it., 1971, I, 1060.

alla riservatezza. Facendo leva su previsioni dettate da diverse disposizioni<sup>140</sup>, in cui riscontrava espressioni di un più generale diritto alla tutela dell'intimità della sfera privata, la giurisprudenza aveva affermato la riconducibilità tra i diritti inviolabili dell'uomo tutelati dall'art. 2 Cost. del diritto alla riservatezza inteso come “*potere dell'interessato di vietare comportamenti di terzi volti a conoscere o far conoscere situazioni o vicende della propria vita personale o familiare, anche se svoltesi al di fuori del recinto domestico, che non avessero un interesse socialmente apprezzabile*”<sup>141</sup>.

Si tratta dunque di un diritto riconducibile alla ristretta cerchia dei diritti della personalità definibile come diritto di tenere segreti aspetti, comportamenti, atti, relativi alla sfera intima della persona. È all'inizio degli anni '50 che prende linfa vitale il dibattito sull'affermazione o meno dell'esistenza di un diritto alla riservatezza.

Il Tribunale di Roma, pur dovendo decidere in merito ai limiti della libertà di espressione artistica, è giunto ad affermare con la sentenza del 14 settembre 1953 l'esistenza nel nostro ordinamento di un “*diritto alla riservatezza che si concreta nel divieto di qualsiasi ingerenza e indiscrezione da parte di terzi nella sfera della vita privata della persona.*”

La Corte di Cassazione, intervenendo sul medesimo caso affrontato dal Tribunale di Roma nel 1953, con la sentenza del 22 dicembre 1956 n. 4487 ha negato l'esistenza di un diritto assoluto al rispetto dell'intimità della vita privata<sup>142</sup>, ritenendo sufficiente rifarsi al principio di cui all'art. 2043 c.c.

Sul tema è ritornata la Corte di Cassazione con la sentenza del 20 aprile 1963 n. 990. Il settimanale “Tempo”, in una serie di articoli, aveva pubblicato diversi particolari sulla vita intima dell'amante del Duce, Claretta Petacci. Gli articoli avevano diffuso descrizioni ritenute offensive nei confronti dei congiunti della Petacci, che hanno intentato una causa al settimanale. La Corte, in questo caso, ha emesso una sentenza decisiva che ha mutato la rigida posizione iniziale adottata su questo tema,

---

<sup>140</sup> Gli artt. 13, 14, 15 Cost. sanciscono diritti che abbracciano le libertà individuali, ossia rispettivamente la libertà personale, di domicilio e la libertà e la segretezza della corrispondenza; l'art. 615 bis c.p. sanziona il comportamento di “*chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentisi nei luoghi indicati nell'art. 614*” ossia luoghi di dimora privata o nelle appartenenze di essi; l'art. 10 c.c. impone all'autorità giudiziaria, su richiesta dell'interessato che si ritenga leso nel decoro o nella sua reputazione, di disporre la cessazione dell'abuso dell'immagine altrui, salvo il risarcimento del danno, gli artt. 96 e 97 l. 633/41 sanciscono i diritti relativi al ritratto di una persona, che non può essere riprodotto, esposto o messo in commercio senza il consenso di quest'ultima, a meno che la riproduzione non sia giustificata da notorietà o dall'ufficio pubblico ricoperto.

<sup>141</sup> TORRENTE A. – SCHLESINGER P., *Manuale di diritto privato*, Milano, 2015.

<sup>142</sup> Nella sentenza si legge: “*nessuna disposizione di legge autorizza a ritenere che sia sancito, come principio generale, il rispetto assoluto dell'intimità della vita privata, tanto meno come limite della libertà dell'arte, salvo che l'operato dell'agente, offendendo l'onore o il decoro o la reputazione della persona, ricada nello schema generale del fatto illecito. Il semplice desiderio di riserbo non è stato ritenuto dal legislatore quale interesse tutelabile fuori dai casi in cui è riconosciuto espressamente un diritto della personalità*”.

pur non sancendo la configurabilità del diritto alla riservatezza. In essa si legge che è riconosciuta *“l’esistenza nel nostro ordinamento di un diritto assoluto di libera determinazione nello svolgimento della personalità, diritto che può ritenersi violato quando si divulgano notizie della vita privata di un soggetto senza il suo consenso, almeno implicito”*.

È la Cassazione a sancire definitivamente, con la sentenza del 27 maggio 1975 n. 2129, l’esistenza di un autonomo diritto alla riservatezza<sup>143</sup>.

Con tale pronuncia, la Cassazione ha adottato una decisa e diretta posizione nei confronti del diritto alla riservatezza. Dopo aver negato per molto tempo l'ammissibilità di una protezione autonoma del rispetto della vita privata, il Supremo Collegio, conformandosi a una copiosa giurisprudenza di merito, è giunto a riconoscere che l'ordinamento giuridico ammette e tutela l'interesse di ciascuno a che non siano resi noti fatti o avvenimenti di carattere riservato senza il proprio consenso. La sentenza afferma che costituisce lesione della privacy la divulgazione di immagini o avvenimenti non direttamente rilevanti per l'opinione pubblica, anche quando tale divulgazione venga effettuata con mezzi leciti e per fini non esclusivamente speculativi. Così si legge nella pronuncia concernente una delle controversie instaurate dall'ex imperatrice dell'Iran, Soraya Esfandiari, contro alcuni giornali che avevano pubblicato delle fotografie che la ritraevano in atteggiamenti intimi con un uomo, nelle mura della sua abitazione<sup>144</sup>. Secondo l'accezione accolta dalla Corte di Cassazione nella sentenza del 1975 n. 2199, il diritto alla riservatezza si identifica dunque con l'interesse a sottrarre alla conoscenza altrui le vicende private, verificatesi dentro e fuori del domicilio domestico, che non abbiano per i terzi un interesse socialmente rilevante. Ed è proprio in tale significato che anche la Corte costituzionale, nella sentenza n. 38 del 1973, aveva annoverato la fattispecie nell'ambito dei diritti inviolabili dell'uomo. Con la pronuncia del 1973, cui sostanzialmente la Corte di Cassazione si è uniformata, il diritto in esame è collocato tra quelli inviolabili dell'uomo garantiti costituzionalmente, richiamandosi anche all'art. 12 della Dichiarazione Universale dei diritti dell'uomo e all'art. 8 della Convenzione europea dei diritti dell'uomo. Afferma la Corte: *“Non contrastano con le norme costituzionali ed anzi mirano a realizzare i fini dell’art.2 affermati anche negli art.3, comma 2, e 13, comma 1, che riconoscono e garantiscono i diritti inviolabili dell’uomo, fra i quali rientra quello del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza, intimità e reputazione, sanciti espressamente negli art. 8 e 10 della Convenzione Europea sui diritti dell’uomo, gli art. 10 c.c., 96 e 97 L. 22/04/1941 n.633”*.

---

<sup>143</sup> Si veda sulla ricostruzione del diritto di riservatezza CARDACI F. – OLIVETTI S., *Il diritto alla riservatezza in Italia*, in <http://www.jus.unitn.it/>.

<sup>144</sup> SALIOLA S., *Il caso Soraya e l'applicazione diretta della CEDU*, su <http://www.iurisprudentes.it/>.

Mentre in Italia il dibattito sulla privacy portava all'affermazione di un pieno riconoscimento della riservatezza quale diritto di tutelare la propria vita intima contro ingerenze varie, anche a livello europeo si facevano progressi.

Nella prospettiva europea il diritto alla privacy è sentito come un diritto fondamentale. In particolare, l'art. 8.1 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (di seguito CEDU), approvata dal Consiglio d'Europa nel 1950, dispone che *“ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza”*. La tutela riconosciuta dalla CEDU non si arresta alla protezione della sfera privata, ma riguarda anche tutto ciò che l'essere umano svolge al di là delle mura domestiche, comprendendo dunque anche la vita professionale. In questo senso si è espressa la Corte europea dei diritti umani statuendo che *“del rispetto della vita privata deve far parte in certa misura il diritto di stabilire relazioni con altri esseri umani. Non sembra esservi alcuna ragione di principio per la quale si debba considerare tale interpretazione della nozione di vita privata tale da escludere attività di natura professionale o commerciale, giacché dopo tutto è nel corso della propria vita lavorativa che la maggior parte delle persone ha una possibilità significativa di sviluppare relazioni con il mondo esterno”*<sup>145</sup>.

Dopo la Convenzione di Strasburgo, contenente un'enunciazione di principi cui dovrebbero (o almeno, avrebbero dovuto) conformarsi le varie legislazioni nazionali, in modo da assicurare il rispetto del diritto alla privacy degli individui nei confronti di ogni elaborazione automatizzata di dati concernenti soggetti identificati o identificabili, e le singole interpretazioni degli Stati nazionali, la tutela della riservatezza come protezione dei dati personali è stata ribadita in tutta una serie di provvedimenti comunitari: la direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, la direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, in seguito abrogata dalla direttiva 2002/58/CE in merito al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni, a sua volta modificata nel 2009.

Le direttive comunitarie in questione avevano come obiettivo quello di conciliare le esigenze della realizzazione del mercato interno con quelle sottese alla tutela della privacy delle persone fisiche. In particolare assicuravano che i dati personali fossero trattati in modo da garantire il rispetto dei diritti e delle libertà fondamentali degli interessati: esse sancivano definitivamente l'esistenza di un

---

<sup>145</sup> Questo principio è stato affermato nel caso *Niemietz contro Germania*, riguardante una perquisizione dell'ufficio di un lavoratore eseguito da una Autorità governativa. Corte EDU, *Niemietz contro Germania*, 16 dicembre 1992, Grande Camera, ricorso n. 13710/88, su <https://hudoc.echr.coe.int/>.

"diritto alla protezione dei dati di carattere personale" distinto e autonomo dal "diritto alla riservatezza". Tuttavia la regolamentazione da esse contenuta non prevedeva una specifica normativa per il trattamento dei dati personali nel lavoro, limitandosi ad incoraggiare l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione delle disposizioni generali della direttiva in funzione delle specificità settoriali<sup>146</sup>.

La necessità di adempiere agli obblighi scaturenti dal diritto internazionale e comunitario e quella di dare attuazione alla direttiva dell'Unione Europea 95/46/CE hanno portato all'adozione della l. n. 675/1996 che, oltre a contenere una disciplina generale per la tutela della privacy nel trattamento dei dati personali, ha istituito la figura del Garante per la protezione di quegli stessi dati<sup>147</sup>. La legge del 1996 è stata successivamente abrogata e sostituita dal d.lgs. n. 196/2003, entrato in vigore il 1° gennaio 2004 e precisamente denominato dal Legislatore "*Codice in materia di protezione dei dati personali*".

Prima della sua modifica intervenuta nel 2018 per rafforzare ulteriormente la protezione delle persone fisiche in merito al trattamento dei dati personali, che in seguito si vaglierà, ma che, si può anticipare, ha determinato l'abrogazione di diversi articoli del Codice privacy, quest'ultimo era composto da tre parti: la prima contenente disposizioni generali applicabili a qualsiasi tipo di trattamento (Titolo III, Capo I), salvo eventuali singole disposizioni particolarmente dettate per i trattamenti effettuati da soggetti pubblici (Titolo III, Capo II) e privati (Titolo III, Capo III); la seconda inerente i trattamenti effettuati in settori specifici, con funzione integrativa o eccettuativa rispetto alle disposizioni contenute nella prima parte, e l'ultima, infine, era dedicata ai meccanismi di tutela amministrativa e giurisdizionale (Titolo I), alle regole di funzionamento dell'Autorità garante preposta alla protezione dei dati personali (Titolo II) e al riordino dell'apparato sanzionatorio (Titolo III)<sup>148</sup>. Nel fornire un profilo esaustivo dell'impianto originario del Codice privacy, occorre citare anche i suoi allegati: il disciplinare contenente la descrizione delle misure minime di sicurezza (All. B), nella loro adozione obbligatorie per i titolari del trattamento, nonché i codici deontologici in materia di giornalismo (All. A1), di ricerca storica (All. A2) e statistica pubblica (All. A3). Era infine espressamente prevista l'allegazione di codici di deontologia e buona condotta non ancora emanati al momento dell'entrata in vigore del Codice.

---

<sup>146</sup> In questo senso l'art. 27 direttiva n. 95/46/CE.

<sup>147</sup> L'art. 154 del Codice privacy, riprendendo in parte l'art. 31 della l. n. 675/1996, attribuisce al Garante molteplici funzioni: di controllo volte alla verifica delle liceità e correttezza dei trattamenti a tutela dei diritti del cittadino rispetto all'elaborazione altrui dei dati che lo riguardano, interdittiva volta all'adozione dei provvedimenti previsti dalla legge o dai regolamenti, promozionale esplicata dal Garante per curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati. Vi si aggiungono poi funzioni consultive e propositive.

<sup>148</sup> KIRSCHEN S., *Il codice della privacy, fra tradizione ed innovazione*, in PANETTA R. (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006.

Il Codice ha rappresentato il punto di arrivo di un'evoluzione iniziata con il riconoscimento giurisprudenziale dei diritti alla riservatezza e all'identità personale<sup>149</sup>, e poi proseguita con la l. n. 675/1996. Arrestarsi qui sarebbe però riduttivo, dovendosi considerare il Codice anche come l'apertura di un nuovo capitolo per la teoria e la prassi dei diritti fondamentali nell'esperienza italiana<sup>150</sup>. Anche a livello contenutistico, il diritto alla riservatezza è stato ampliato da dottrina e giurisprudenza evidenziando che *“il soggetto non ha più diritto a che in assoluto di sé si sappia, mentre ha certamente diritto a conoscere che cosa, perché e come di sé si sa”*<sup>151</sup>.

Culmine di questo sviluppo è l'affermazione di un *“diritto alla protezione dei dati personali”*<sup>152</sup>, qualificato come diritto fondamentale dall'art. 8<sup>153</sup> della Carta dei diritti fondamentali dell'Unione Europea<sup>154</sup>. La Carta distingue la protezione dei dati sia dal diritto di ogni individuo al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni, sancito dall'art. 7<sup>155</sup>, sia dalla precisazione posta dall'art. 11, secondo il quale la libertà di espressione e d'informazione include la libertà di opinione e la libertà di ricevere e di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. La tutela della privacy riceve così, per effetto della proclamazione della Carta di Nizza, un notevole contributo.

In conclusione di questa breve disamina e alla luce degli apporti normativi comunitari e internazionali, non è celabile dunque l'emersione di un "nuovo" diritto alla privacy, come fattispecie complessa, rispetto alla quale diritto alla riservatezza, diritto all'identità personale e

---

<sup>149</sup> Cass., 27 maggio 1975, n. 2129, su <https://protezionedatipersonali.it>: *“deve ritenersi esistente nel nostro Ordinamento un generale diritto della persona alla riservatezza, inteso alla tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi al di fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le esigenze che (...) non siano giustificate da interessi pubblici preminenti”*.

<sup>150</sup> RESTA G., *Il diritto alla protezione dei dati personali*, in CARDARELLI F. - SICA S. - ZENO-ZENCOVICH V. (a cura di), *Il codice dei dati personali, temi e problemi*, Milano, 2004.

<sup>151</sup> BARRACO E. – STIZIA A., *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milanofiori Assago (MI), 2016.

<sup>152</sup> L'originario art. 1 Codice privacy affermava: *“chiunque ha diritto alla protezione dei dati personali”*.

<sup>153</sup> Art. 8.1 della Carta dei Diritti fondamentali dell'Unione Europea, con rubrica *“protezione dei dati di carattere personale”*:

*Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.*

*Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.*

*Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*

<sup>154</sup> La Carta dei diritti fondamentali dell'Unione europea è stata proclamata ufficialmente a Nizza il 7 dicembre 2000 da Parlamento, Commissione e Consiglio europeo.

<sup>155</sup> Art.7 Carta dei Diritti fondamentali dell'Unione Europea, rubricato *“Rispetto della vita privata e della vita familiare”*:

*“Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni”*.

diritto alla protezione dei dati personali si attecchiano a singole componenti, tutte dotate di pari dignità costituzionale<sup>156</sup>.

---

<sup>156</sup> VARANI E., *Il "nuovo diritto "alla privacy. Dalla Carta di Nizza al "Codice in materia di protezione dei dati personali"*, su <https://www.filodiritto.com/>.

## CAPITOLO II

### IL CONTROLLO A DISTANZA ALLA LUCE DEL JOBS ACT

#### 1. Esigenze di riforma: il contesto che fa da innesco all'art. 23 del d.lgs. n. 151/2015

La sorveglianza e il controllo, come emerso dal capitolo precedente, non nascono oggi ma sono strutturali al capitalismo e alla tecnica quali forme di organizzazione della vita.

Nell'odierna società tecno-capitalista ci sono tuttavia differenze importanti rispetto al passato che vanno evidenziate. In primis, oggi non sono più gli Stati a controllare e profilare gli individui, ma le società private (dalla Fiat a Facebook); in secondo luogo, la tecnologia ha abilitato il passaggio da una sorveglianza mirata, e quindi limitata, a una sorveglianza generalizzata e per di più a volte volontaria, anche se indotta da un modello di business creato per far credere di essere liberi quanto più si condivide.

La forma perfetta di controllo si è realizzata, evidentemente, grazie alle nuove tecnologie<sup>157</sup>.

Al momento della sua emanazione lo Statuto dei lavoratori è apparso di grande attualità, dotato di un innegabile impatto innovativo. Tuttavia, nonostante risultasse stare al passo con i tempi, il contesto in cui era nato era quello di una realtà *in fieri*, destinata a evolversi rapidamente, specie a livello tecnologico, come dimostrato da vari episodi nel frattempo intervenuti: era stato sviluppato e prodotto l'Olivetti Programma 101 (sigla P101), il primo "desktop computer" commerciale programmabile, motivo per cui viene definito anche come il primo "personal computer" della storia, la missione spaziale Apollo 8 era da poco rientrata sulla Terra, dopo aver effettuato 10 orbite intorno alla Luna e aver inviato le prime immagini della Terra viste dal lato del nostro satellite, l'uomo era stato sulla Luna, era stato realizzato il primo microprocessore dall'italiano Federico Faggin, l'invenzione della ET 101, la prima macchina da scrivere completamente elettronica su scala mondiale, aveva posto l'Italia in vetta nell'alta tecnologia, l'avvento e la diffusione di Internet e dei suoi servizi hanno rappresentato una vera e propria rivoluzione tecnologica e socio-culturale dagli inizi degli anni novanta (assieme ad altre invenzioni come i telefoni cellulari), nonché uno dei motori dello sviluppo economico mondiale nell'ambito delle Tecnologie dell'Informazione e della Comunicazione (ICT), il 29 novembre 2010 è stato proposto per la prima volta nell'ordinamento italiano il riconoscimento del diritto di accesso ad Internet come diritto fondamentale dal giurista

---

<sup>157</sup> DEMICHELIS L., *Sorvegliati e contenti: così i social hanno realizzato la forma di controllo perfetta*, su [www.agendadigitale.eu/cultura-digitale/](http://www.agendadigitale.eu/cultura-digitale/).

Stefano Rodotà<sup>158</sup>, per concludere con il 2011, anno in cui la connessione alla rete è stata qualificata dall'ONU come diritto umano.

Tutto ciò è stato prova dell'incessante progresso tecnologico, cui si stava e si sta assistendo, destinato a rivoluzionare qualunque campo, soprattutto quello lavorativo.

Inoltre, se, in passato, il datore di lavoro poteva attuare un Grande Fratello nei confronti dei lavoratori mediante l'ausilio delle telecamere, a distanza di cinquanta anni le telecamere sono diventate l'ultimo strumento di cui temere, sono forme di controllo non occulto, e per questa ragione a esse spesso i datori di lavoro preferiscono le telecamere di ultima generazione, estremamente piccole che, pur essendo in funzione, all'occhio umano appaiono spente, o addirittura strumenti di controllo non visibili che consentono la geo-localizzazione e la tracciatura delle attività.

Il diverso livello di timore impresso dall'impiego datoriale delle telecamere nei lavoratori degli anni '70 e nei lavoratori del nuovo millennio è un'altra spia dei progressi informatici, nonché dell'emersione di una casistica e di fattispecie del tutto nuove, che il legislatore del 1970 non poteva neanche lontanamente immaginare.

Questa evoluzione dei tempi, insieme all'inarrestabile informatizzazione dei luoghi di lavoro, ha evidenziato l'obsolescenza contro la quale inevitabilmente si sarebbe scontrata, o meglio si stava già scontrando, la normativa statutaria; e in particolare l'art. 4 St. lav. che, con la sua rubrica originaria "*impianti audiovisivi*", alla luce della carrellata di eventi poc'anzi ricostruita, fotografava una realtà destinata a trasformarsi.

L'evoluzione tecnologica posteriore allo Statuto dei lavoratori ha reso inevitabile una rivisitazione normativa della disciplina regolatrice in tema di controlli, sia per la limitatezza della norma legale, troppo ancorata al contesto di cui era figlia, incapace perciò di ricomprendere le forme di controllo nate successivamente e diverse da quelle già presenti, sia per la necessità di una armonizzazione alle disposizioni del codice della privacy.

La società dell'informazione ha elaborato modelli di produzione e di organizzazione del lavoro, che, rispetto a quello tayloristico, hanno fatto emergere esigenze di controllo dell'attività dei lavoratori, fino a qualche tempo fa, impensabili e alle quali è spesso materialmente impossibile far

---

<sup>158</sup> Il giurista Stefano Rodotà, nell'ambito dell'Internet Governance Forum Italia a Roma, aveva proposto di inserire un articolo "21-bis" secondo cui: "*tutti hanno eguale diritto di accedere alla rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale. La legge stabilisce provvedimenti adeguati a prevenire le violazioni dei diritti di cui al Titolo I della parte I*". Si trattava quindi di una modifica che prevedeva l'inserimento del diritto di accesso a Internet in stretto legame con il principio di uguaglianza di cui all'art. 3 Cost. e con un legame particolare alla libertà di espressione.

fronte attraverso le modalità tradizionali di controllo, tipiche del contesto produttivo e organizzativo dell'epoca in cui lo Statuto dei lavoratori ha visto la luce<sup>159</sup>.

Oggi le forme di controllo sono infinite, quotidianamente si sviluppano e nascono nuovi strumenti, sensori di presenza fisica, impianti di monitoraggio a distanza, sistemi di videosorveglianza intelligente, braccialetti elettronici indossabili per la rilevazione dei movimenti fisici e software in grado di misurare i tempi di ogni attività lavorativa. E non solo. Ormai è cristallino che le strumentazioni tecnologiche diffuse in molteplici contesti lavorativi, ove possono risultare necessarie per l'espletamento della prestazione lavorativa, sono allo stesso tempo strumenti che consentono *“il monitoraggio costante delle attività lavorative nonché l'immagazzinamento di grandi quantità di dati sugli utilizzatori, accentuando di gran misura il rischio per il lavoratore di essere sottoposto a controlli occulti e invasivi”*<sup>160</sup>.

Il progresso tecnologico ha reso dunque i confini sensibilmente labili. Ecco che diventa più pregnante il dibattito avente a oggetto la determinazione dei limiti del potere di controllo del datore di lavoro.

## **2. L'articolo 4 dello Statuto dei lavoratori come effetto del Jobs Act**

Ricostruito il quadro di riferimento, si può passare alla disamina del nuovo art. 4 St. lav., per come riformato dall'art. 23 d.lgs. n. 151/2015<sup>161</sup>, di cui si è servito il Legislatore per innovare sensibilmente la disciplina in una prospettiva di semplificazione. Con la l. n. 183/2014 il Legislatore ha infatti delegato il Governo a emanare uno o più decreti legislativi, con i quali compiere *“una revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive e organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore”*<sup>162</sup>.

È possibile identificare due nuclei normativi, che, per chiarezza espositiva, si andranno a esaminare separatamente, tenendo a mente la loro insita connessione.

Il primo nucleo raccoglie le norme, collocate nel primo e nel secondo comma della disposizione statutaria, rivolte a disciplinare la possibilità per il datore di lavoro di installare strumenti di controllo a distanza.

---

<sup>159</sup> BELLAVISTA A., *I poteri dell'imprenditore e la privacy del lavoratore*, in Dir. lav., 2002, I.

<sup>160</sup> RIZZI R.– VENTURA A., *La tutela della privacy del lavoratore controllato a distanza*, Consiglio e La Fondazione Nazionale dei Dottori Commercialisti.

<sup>161</sup> Le nuove norme del Governo di riforma della disciplina del controllo a distanza dei lavoratori sono contenute nel Titolo II (*Disposizioni in materia di rapporto di lavoro e pari opportunità*), Capo I (*Disposizioni in materia di rapporto di lavoro*) all'art. 23 dello schema di decreto legislativo delegato (*Modifiche all'articolo 4 della Legge 20 maggio 1970 n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196*).

<sup>162</sup> Art.1, comma 7 lett. f), della legge delega n. 183/2014.

Distinto dal tema delle regole di installazione è quello dei limiti entro cui il datore di lavoro può accedere alle informazioni registrate dallo strumento ed eventualmente poi avvalersene nell'ambito del rapporto di lavoro. Su questo secondo aspetto il Legislatore è intervenuto con il terzo comma dell'articolo novellato<sup>163</sup>.

## 2.1 La rimodulazione dei controlli: il nuovo comma 1

Prendendo le mosse dal contenuto del primo nucleo delineato poc'anzi, una prima innovazione si riscontra a livello terminologico, si tratta della rubrica.

L'originaria rubrica "*impianti audiovisivi*", espressione utilizzata anche nel corpo del testo stesso, rivelatrice dello scenario tecnologico allora esistente e delle apparecchiature per le quali la norma era stata per la maggiore concepita, ossia telecamere aziendali a circuito chiuso associate alle catene di montaggio, è stata sostituita dalla più ampia "*gli impianti audiovisivi e gli strumenti di controllo*"<sup>164</sup>. L'incipit della disposizione sotto esame, in particolare, parla di "*strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori*". Siamo di fronte a una fattispecie aperta: fermo il rinvio sempre attuale, data la loro proliferazione che si analizzerà a tempo debito, agli impianti audiovisivi, il termine generico "strumenti" deve vedersi riferito a entrambe le componenti di qualsivoglia sistema informatico, l'*hardware*, ossia lo strumento di lavoro, quale il computer, e il *software*, per tale intendendosi i programmi a cui accede il lavoratore, gli applicativi informatici, la cui assenza determinerebbe l'inerzia delle apparecchiature, anche in relazione al compimento di controlli a distanza.

La norma rivela così la sua notevole capacità di adeguamento al progresso tecnologico, come prova l'estesa casistica giurisprudenziale che ha coinvolto la precedente formulazione.

Per riprendere casi della giurisprudenza meno recente, sono stati assoggettati alla disciplina del vecchio art. 4, comma 2, St. lav., ma a una analoga conclusione si dovrebbe giungere anche oggi in riferimento all'attuale comma 1, le telecamere che riprendono anche l'attività dei lavoratori<sup>165</sup>, gli

---

<sup>163</sup> Per un primo commento all'art. 4 St. lav. novellato, cfr. BALLETTI E., *I controlli a distanza dei lavoratori dopo il jobs act*, in SANTONI F. - RICCI M. - SANTUCCI R. (a cura di), *Il diritto del lavoro all'epoca del jobs act*, Napoli, 2016; BELLAVISTA A., *Il nuovo art. 4 dello Statuto dei lavoratori*, in ZILIO GRANDI G. - BIASI M., *Commentario breve alla riforma del "Jobs Act"*, 2016; DEL PUNTA R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23 d.lgs. n. 151/2015)*, in Riv. It. Dir. Lav., 2016, 1, I, pp. 77 ss.; MAIO V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in Arg. Dir. Lav., 2015, 6, pp. 1186 ss.; SALIMBENI M.T., *La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in Riv. It. Dir. Lav., 2015, 4, I, pp. 589 ss.

<sup>164</sup> Cfr. SPEZIALE V., *Le politiche del lavoro del governo Renzi: il Jobs Act e la riforma dei contratti e di altre discipline del rapporto di lavoro*, in WP C.S.D.L.E. "Massimo D'Antona". IT, n. 233/2014, pp. 37 ss.; BELLAVISTA A., *Il controllo sui lavoratori*, Torino, 1995.

<sup>165</sup> Cfr. Cass., 17 giugno 2000, n. 8250, su <https://www.unioncamere.gov.it/>; Cass., 22 ottobre 2002, n. 42217, in Dir. prat. lav., 2002, p. 506.; GOFFREDO M.T. – MELECA V., *Jobs Act e nuovi controlli a distanza*, in Diritto e Pratica del Lavoro 31/2016, p. 1898, elencano alcune apparecchiature che potrebbero essere considerate come strumenti di

scanner che consentono la memorizzazione e la verifica dei dati relativi alle singole casse dei supermercati, e ancora i dischi installati sulle macchine di lavorazione e collegati a un registratore “Kienzle”<sup>166</sup>, su cui rimangono impressi tracciati grafici differenti a seconda delle diverse fasi di funzionamento o di arresto automatico delle macchine, che permettono di valutare *ex post* l’efficienza degli operai, la loro tempestività, e le loro pause eccessive di lavoro<sup>167</sup>.

Del pari rientrano nel *genus* di strumenti, come del resto confluivano nel concetto di apparecchiature in precedenza, le disparate tipologie di software da cui possa derivare un controllo sull’attività dei lavoratori. Già negli anni '80, quando l’informatica cominciava a prendere piede, la giurisprudenza aveva ricondotto alla disciplina limitativa statutaria “*i programmi operanti su elaboratori elettronici, utilizzati in modo da riportare su tabulati il codice di identificazione del singolo addetto al videoterminale unitamente a una serie numerosa di dati che riguardano il funzionamento del computer e che consentono (...) di ottenere un quadro estremamente analitico dei tempi e delle modalità di svolgimento della prestazione lavorativa*”<sup>168</sup>.

E ancora si considerino i sistemi informatici di rilevazione automatica, in tempo reale, delle operazioni di sportello<sup>169</sup>, e i diffusi programmi informatici di monitoraggio della posta elettronica e degli accessi a internet<sup>170</sup>.

Al di fuori della fattispecie regolatoria dell’art. 4 St. lav. residua, da un lato, un’area di totale illiceità, rappresentata dall’installazione e dall’impiego di strumenti che abbiano l’esclusiva funzione di controllare a distanza l’attività dei lavoratori, senza soddisfare alcuna esigenza organizzativa, produttiva, di sicurezza del lavoro e, oggi, anche di tutela del patrimonio aziendale. Dall’altro, rimane un’area di piena legittimità, costituita da tutti quegli strumenti di utilità aziendale, dai quali non derivi alcuna possibilità di una sorveglianza a distanza sull’attività dei dipendenti. Così è, ad esempio, per gli strumenti di controllo statistico della produzione, rientrante nei processi di “qualità totale” o di raccolta dei dati quantitativi della stessa; o, ancora per i sistemi di accesso all’archivio

---

controllo, rientranti nell’alveo del nuovo comma 1: telecamere e webcam installate all’interno degli edifici lavorativi e loro eventuali pertinenze, come aree di parcheggio, per esigenze organizzative, produttive, di sicurezza del lavoro o del patrimonio aziendale idonee a riprendere l’attività dei lavoratori, sistemi di geo-localizzazione installati su veicoli utilizzati da più lavoratori, centralino telefonico elettronico, registratori di cassa elettronici, telefoni cellulari usati senza codici personali da più lavoratori ecc.

<sup>166</sup> Cfr. Cass. 18 febbraio 1983, n. 1236, in Giust. civ., 1983, I, 1755; Pret. Milano, 4 ottobre 1988 in Not. giurispr. lav. 1989, 436.

<sup>167</sup> Pret. Firenze, 20 marzo 1990, in Orient. giur. lav., 1993, p. 5.

<sup>168</sup> Pret. Milano, 5 dicembre 1984, in Foro it., 1985, p. 285.

<sup>169</sup> Cass. 9 febbraio 2016, n.2531, su <https://www.studiocerbone.com/>.

<sup>170</sup> Cfr. Cass. 23 febbraio 2010 n. 4375, su <https://www.ricercagiuridica.com/>; Cass. 23 febbraio 2012 n. 2722, su <http://www.avvocatomandico.it/>.

informatico condiviso dai dipendenti e dall'impresa, non differendo dalla consultazione di un archivio cartaceo in cui sia riposta la documentazione formata da ciascun lavoratore<sup>171</sup>.

Procedendo con la disamina della struttura della norma, se l'originario comma 1 dell'art. 4 St. lav. esplicitava, come precedentemente visto, un divieto assoluto di controllo intenzionale, la nuova disposizione apparentemente non prevede più tale divieto, non avendo l'art. 23 del d.lgs. 151/2015 mantenuto nella disposizione statutaria l'affermazione del principio generale che in precedenza ne costituiva e, l'apertura e, l'indicazione programmatica.

Tuttavia non vi è dubbio che la scelta del Legislatore delegato di non mantenere nel nuovo impianto normativo l'espreso divieto non implichi come inevitabile conseguenza la totale ammissione di un controllo a distanza senza limiti sull'attività dei lavoratori, sotto la vigenza del nuovo art. 4 St. lav. Viene infatti ora dettato al comma 1 che *“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”*.

Il divieto di controlli a distanza del tutto liberalizzati sull'attività dei lavoratori è implicitamente conservato dalla struttura lessicale del comma, venendo ricavato *a contrario*.

L'impiego dell'avverbio *esclusivamente* è indice rivelatore di come l'installazione di strumenti in grado di consentire il controllo a distanza sui lavoratori non sia ammessa per qualsiasi finalità, ma solo per quelle espressamente indicate, le uniche legittimanti l'uso di strumenti potenzialmente intrusivi<sup>172</sup>. Ne deriva che la condotta datoriale di predisposizione di un sistema di controllo orientato al solo controllo della prestazione resa dai propri dipendenti sarebbe affetta da illegittimità<sup>173</sup>.

Appare quindi corretto ritenere ancora vivo, con il nuovo art. 4 St. lav., così come nel 1970, il divieto di ricorrere a strumenti tecnologici al solo scopo di controllare l'attività lavorativa dei dipendenti.

---

<sup>171</sup> Pret. Milano 1 marzo 1993 in Orient. giur. lav., 1994.

<sup>172</sup> LISO F., *Brevi osservazioni sulla revisione della disciplina delle mansioni contenuta nel decreto legislativo n° 81/2015 e su alcune recenti tendenze di politica legislativa in materia di rapporto di lavoro* in Working Papers “Massimo D’Antona” n. 257/2015, in <http://csdle.lex.unict.it>.

<sup>173</sup> Tale precisazione ridimensiona i timori manifestati nelle more del procedimento di formazione legislativa da parte di alcuni esponenti sindacali; si ricorda il grido d'allarme levato il 18 giugno 2015, all'indomani della pubblicazione dello schema di decreto legislativo a opera del Governo, da parte del Segretario Generale della CGIL, che, denunciando un abuso rispetto alle norme di diritto esistenti sulla privacy delle persone, parlava della nuova norma come di *“uno spionaggio nei confronti dei lavoratori. Se uno viene autorizzato a entrare nei mezzi di comunicazione che usano le persone, è difficile non definirlo Grande Fratello”* (cfr. *Jobs Act, controlli a distanza su pc e telefonini. La Cgil: “un colpo di mano”* in Repubblica.it, 18 giugno 2015).

Anche la categoria dei controlli preterintenzionali è stata mantenuta ferma, tanto che a tal proposito, il nuovo art. 4 St. lav., ricalcando in parte il testo del precedente comma 2, replica l'impianto tradizionale, per cui alla regola del divieto dei controlli a distanza intenzionali fanno eccezione quei controlli a cui il Legislatore, nel 1970, aveva correlato una finalità produttiva, organizzativa o legata alla sicurezza. Il Legislatore ha dunque scelto di far confluire le discipline di entrambe le tipologie di controllo in un unico comma.

Tuttavia, sin da subito, il Legislatore introduce una novità consistente nell'affiancare l'esigenza di tutela del patrimonio, non presente nel testo originario dell'art. 4 St. lav., alle tradizionali esigenze organizzativo – produttive e della sicurezza sul lavoro<sup>174</sup>. E a tal proposito, per terminare questa iniziale disamina, è opportuno richiamare l'attenzione sull'assoluta innovazione del nuovo primo comma, ossia quella dei c.d. controlli difensivi.

L'esplicitazione della tutela del patrimonio aziendale individua chiaramente la categoria dei controlli difensivi che, come quelli occasionati da esigenze organizzative, produttive o di sicurezza del lavoro, ossia i controlli preterintenzionali, viene sottoposta ai limiti di cui all'art. 4 St. lav.

In questo modo, ossia tramite l'inserimento di una nuova finalità tra le ragioni giustificatrici di un controllo, la riforma è diventata autrice di una “*giuridificazione dei controlli a distanza difensivi*”<sup>175</sup>, ricondotti dal Legislatore nella categoria dei controlli preterintenzionali. Questi ultimi del resto hanno in comune con i controlli difensivi il consentire almeno potenzialmente e in via riflessa un monitoraggio anche dell'attività lavorativa. Pur essendo tale possibilità indiretta, giacché non costituisce il primario scopo del datore di lavoro, ha comunque una consistenza realistica, dovuta all'uso da parte dell'imprenditore della strumentazione tecnica, con cui si esplica il controllo a distanza. Tra l'altro, l'utilizzo di apparecchiature informatiche accentua ulteriormente la potenzialità di sorveglianza per la loro capacità di raccogliere e trattare un elevato numero di dati, anche contemporaneamente.

Emerge una stretta connessione tra le due tipologie di controlli ed è per questa ragione che è stata ipotizzata una riconducibilità dei controlli difensivi nella categoria di quelli preterintenzionali. Come visto, prima della modifica dell'art. 4 St. lav., secondo giurisprudenza consolidata, il datore di lavoro non doveva rispettare la procedura di cui all'art. 4, comma 2, St. lav. per controllare se i lavoratori avessero commesso illeciti lesivi di beni estranei al rapporto di lavoro, comprensivi anche del patrimonio aziendale.

---

<sup>174</sup> COSATTINI L. A., *Le modifiche all'art. 4 Stat. Lav. sui controlli a distanza, tanto rumore; per nulla?*, in *Lav. giur.*, n. 11/2015, 985.

<sup>175</sup> LEVI A., *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei lavoratori dopo il Jobs Act*, Milano, 2016.

Poiché l'accordo sindacale o l'autorizzazione amministrativa sono oggi richiesti anche per installare impianti o apparecchiature per ragioni di tutela del patrimonio aziendale, le due categorie di controllo difensivo e preterintenzionale sembrano andare a sovrapporsi.

Sulla scia di tale impostazione non sopravviverebbe più alcuno spazio per controlli difensivi totalmente esclusi dal campo operativo dell'art. 4 St. lav.

Viene così offerta una soluzione rigida che non consentirebbe più di eludere le procedure della disposizione in questione, pure laddove si voglia tutelare "beni estranei a rapporto di lavoro", eliminando ogni difficoltà pratica di delimitazione dei confini.

Se la rigidità della nuova formulazione è da ritenersi "portatrice di chiarezza e semplificazione", essendo ora cristallino che gli strumenti di controllo dai quali possa derivare un controllo a distanza non possono essere utilizzati se non per gli scopi previsti dalla legge<sup>176</sup>, emergono alcune perplessità.

Va infatti sottolineato che la rigidità del nuovo comma 1 emerge anche dall'uso dell'espressione "patrimonio aziendale".

Come rilevato in dottrina, tale nozione ricomprende sia i beni materiali, sia quelli immateriali dell'impresa e, quindi, ogni rapporto essenziale allo svolgimento dell'attività produttiva<sup>177</sup>. Sulla base di ciò, si era arrivati a costruire una equilibrata interpretazione, che avrebbe permesso di raggiungere quel bilanciamento di interessi tra difesa del patrimonio aziendale e tutela del diritto alla privacy tanto cercato. Era stato detto, infatti, che, utilizzando una concezione ampia di patrimonio aziendale, comprensiva anche del bene dell'efficienza aziendale, si sarebbe potuto distinguere tra controlli difensivi estranei all'art. 4 St. lav., e quindi sempre leciti, perché posti in essere in occasione di condotte del dipendente lesive della produttività dell'impresa, ossia della sua capacità produttiva, e controlli occasionati da condotte del dipendente lesive solo della produzione e, pertanto, rientranti nell'ambito di applicazione dell'art. 4 St. lav. Tale lettura, alla luce dell'articolo riformato, non sembra essere più praticabile. Anche in caso di danno alla produttività, di lesione di profili estranei al rapporto di lavoro, di condotte che investano il patrimonio aziendale, l'uso di strumenti di controllo dovrà sempre essere soggetto all'art. 4, comma 1, St. lav.

Tra l'altro una formulazione così rigida, anche in considerazione della natura penalistica che l'art. 4 possiede tutt'ora, mette a rischio la possibilità di configurare controlli difensivi legittimi perché

---

<sup>176</sup> SALIMBENI M.T., *La riforma dell'art. 4 dello statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in Riv. it. dir. lav., 2015, n.4, p. 589.

<sup>177</sup> Cfr. ALVINO I., *L'articolo 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica*, in Dir. rel. ind., 2014, n. 4, pp. 999 ss.; LEVI A., *Il controllo informatico sull'attività del lavoratore*, Torino, 2013; SPINELLI G., *La legittimità dei controlli datoriali cd. "difensivi": certezze apparenti in una categoria dubbia*, in Riv. it. dir. lav., 2013, n.1, II, 2016.

finalizzati a provare illeciti penali. Ciò in quanto è indubbio che, laddove il reato vada a ledere il patrimonio aziendale (situazione configurabile, ad esempio, nel caso di una cassiera che sottragga il denaro incassato del supermercato-datore di lavoro), l'eventuale controllo difensivo sarebbe finalizzato alla tutela del patrimonio aziendale stesso, e, allora, attualmente necessiterebbe dell'espletamento della procedura sindacale – amministrativa di cui all'art.4 St. lav.

Tuttavia, nel tentativo di prevedere alcuni esiti applicativi, è ragionevole ritenere che la giurisprudenza penale manterrà la propria posizione, continuando a ritenere legittimo il controllo difensivo tramite il quale si rilevi l'esistenza di un reato, dando prevalenza all'interesse pubblico rispetto a quello della riservatezza del lavoratore. Una soluzione diversa condurrebbe a esiti aberranti sotto il profilo della giustizia sostanziale, creando una sorta di immunità per i lavoratori che si rendano responsabili di illeciti penali lesivi del patrimonio aziendale.

In definitiva non sembra dunque che la nuova formulazione dell'art. 4 St. lav. abbia fornito una soluzione del tutto equilibrata al conflitto di interessi tra datore e dipendente<sup>178</sup>.

## 2.2 Le novità procedurali

Nel nuovo art. 4 St. lav. è stata confermata la scelta di procedimentalizzare i poteri del datore di lavoro in materia di controlli a distanza *“garantendo quindi nel sistema rinnovato la storica “centralità” al procedimento di controllo (sindacale o amministrativo)”*<sup>179</sup>.

Ecco che l'articolo novellato procede disponendo, sempre nel primo comma, senza discostarsi molto dal testo originario esaminato nel capitolo precedente, che gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere installati, oltre che in presenza delle esigenze già richiamate, *“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 primo periodo possono essere installati previa autorizzazione delle sedi territoriali dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi”*.

---

<sup>178</sup> Cfr. TUFO M. in BASENGHI F. – RUSSO A. (a cura di), *Flessibilità, sicurezza e occupazione alla prova del Jobs Act*, Torino, 2016; LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei lavoratori dopo il Jobs Act*, Milano, 2016.

<sup>179</sup> MAINARDI S., *Le relazioni collettive nel “nuovo” diritto del lavoro, relazione nell'ambito delle giornate di studio AIDLASS*, Napoli, 16-17 giugno 2016, dattiloscritto, p. 43.

Il Legislatore ha inciso fortemente sulla procedura autorizzatoria, sindacale o amministrativa, con un preciso obiettivo: la semplificazione. Tale scopo è perseguito attraverso una triplice novità.

A livello degli accordi sindacali, innanzitutto, l'installazione richiede un accordo con la R.S.U. o con le R.S.A., precisazione che rappresenta una novità, giacché nel testo previgente erano menzionate solo le R.S.A. In secondo luogo, nel caso di imprese radicate nel territorio di più province o di più regioni, l'accordo può essere stipulato con le associazioni sindacali comparativamente più rappresentative a livello nazionale. Si tratta di un'innovazione rilevante dal momento che permette alle imprese delocalizzate sul territorio di concludere un unico accordo sul piano nazionale, valido per tutte le unità, garantendo di raggiungere una piena uniformità decisionale.

A livello di procedura amministrativa, in mancanza di accordo<sup>180</sup>, il datore di lavoro può adire direttamente la sede territoriale dell'Ispettorato nazionale del lavoro, o chiedere un'autorizzazione, in caso di imprese con unità produttive dislocate negli ambiti di competenza di più direzioni territoriali del lavoro, alla sede centrale dell'Ispettorato nazionale del lavoro.

Un dubbio che poi è sorto era quello di capire se il previo esperimento di un tentativo di accordo con le R.S.A./ R.S.U. fosse condizione di ammissibilità per presentare l'istanza all'Ispettorato nazionale del lavoro<sup>181</sup>. La tesi dominante propende per la risposta affermativa, qualificando l'avvio di una trattativa sindacale come onere, con la conseguenza che al datore di lavoro resterebbe inibita la possibilità di chiedere l'intervento ministeriale se non in caso di fallimento del tentativo<sup>182</sup>.

---

<sup>180</sup> Il mancato raggiungimento dell'accordo è una situazione che si può concretare in caso di assenza di soggetti sindacali abilitati a stipulare, come avviene, ad es., per imprese con meno di quindici dipendenti, dove non è possibile costituire R.S.A. o R.S.U., o, anche al di sopra dei quindici, se le suddette rappresentanze non siano state costituite.

<sup>181</sup> L'art. 23 del d.lgs. 151/2015 richiedeva, in mancanza di accordo, per l'installazione degli strumenti l'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. Dunque rispetto alla normativa previgente, al posto dell'Ispettorato del lavoro figurava la direzione territoriale del lavoro (Sezione Ispettiva), che da tempo aveva sostituito anche in tale funzione l'Ispettorato del lavoro. Invero, le funzioni dell'Ispettorato del lavoro sono state prima attribuite alla direzione provinciale del lavoro ai sensi dell'art. 6, d.m. 7 novembre 1996, n. 687; in seguito con d.p.r. 7 aprile 2011, n. 144 sono state istituite le direzioni Territoriali del lavoro. Tuttavia l'art. 1 del d.lgs. 149/2015, sulla razionalizzazione e semplificazione dell'attività ispettiva in materia di lavoro e legislazione sociale, ha istituito l'Ispettorato nazionale del lavoro, integrante i servizi ispettivi del Ministero del lavoro e delle politiche sociali, dell'INPS e dell'INAIL. In più l'art. 6, comma 6, d.lgs. 149/2015 afferma che dalla data indicata dai decreti di cui all'articolo 5, comma 1, cessano di operare le direzioni interregionali e territoriali del lavoro e sono attribuiti alle sedi territoriali dell'Ispettorato i compiti già assegnati alle predette direzioni dagli articoli 15 e 16 di cui al decreto del Presidente del Consiglio dei Ministri 14 febbraio 2014, n. 121. Da ultimo il d.lgs. 24 settembre 2016, n. 185, ha eliminato il riferimento alle direzioni territoriali del lavoro o, in caso di aziende nazionali, al Ministero del lavoro, riservando la concessione delle richieste autorizzazioni ai fini dell'uso d'impianti audiovisivi e altri strumenti dai quali possa derivare la possibilità di controllo a distanza dell'attività dei lavoratori alla sola competenza delle sedi territoriali o della sede centrale dell'Ispettorato nazionale del lavoro.

<sup>182</sup> Cfr. CATAUDELLA A., *Commento all'art. 4*, in PROSPERETTI U. (diretto da), *Commentario allo Statuto dei lavoratori*, 1975, Milano, 89; TREU T., *Condotta antisindacale e atti discriminatori*, Franco Angeli, Milano, 1974, p. 72; VENEZIANI B. *Commento agli artt. 4 e 6*, in GIUGNI G. (diretto da), *Lo Statuto dei Lavoratori, Commentario*, Milano, 1979, p. 168.

Se è precisato che l'accordo sindacale atto ad autorizzare l'installazione dell'apparecchiatura è quello stipulato con la R.S.U. o le R.S.A., non è definita la regola di formazione della volontà della rappresentanza e dunque di validità dell'accordo.

Le R.S.U. costituiscono un modello di rappresentanza dei lavoratori in una data azienda, di fonte contrattuale, elettivo e alternativo a quello della R.S.A., in virtù della cd. clausola di salvaguardia<sup>183</sup>, per cui le sigle sindacali che partecipano alle elezioni per le R.S.U. si impegnano a non costituire R.S.A. nella stessa impresa. In presenza di una RSU, in caso di non unanimità all'interno della R.S.U. stessa, si può ritenere operativa la regola maggioritaria prevista dall'accordo istitutivo delle R.S.U.<sup>184</sup>.

Più complesso è il caso delle R.S.A.

Si è ritenuto che se l'azienda rientra tra quelle tenute all'applicazione del Testo Unico sulla Rappresentanza del 10 gennaio del 2014, si potrà invocare la regola dettata nella parte terza del Testo Unico, laddove è prescritto che il contratto debba ritenersi efficace ed esigibile *“se approvato dalle RSA costituite nell'ambito delle associazioni sindacali che, singolarmente o insieme ad altre, risultino destinatarie della maggioranza delle deleghe relative ai contributi sindacali conferite dai lavoratori dell'azienda nell'anno precedente a quello in cui avviene la stipulazione, rilevati e comunicati ai sensi della presente intesa”*.

Laddove l'impresa sia al di fuori dell'ambito di applicazione del Testo Unico, la disposizione non chiarisce se debba valere anche in tal caso la regola maggioritaria, o se l'autorizzazione possa ritenersi valida solo se ottenuta con il consenso di tutte le R.S.A. presenti in azienda.

Il Ministero del Lavoro, tra la regola della maggioranza e quella del consenso di tutte le R.S.A. costituite in azienda, per la validità dell'accordo collettivo si è ad ogni modo espresso a favore della prima<sup>185</sup>.

In merito all'accordo con le rappresentanze sindacali aziendali, si è a lungo discusso circa la sua natura, ossia se dovesse ammettersi la sua bilateralità o se si dovesse interpretare l'originario secondo comma dell'art. 4 St. lav. come attributivo alle R.S.A. di un potere unilaterale di autorizzazione al compimento di un'attività che altrimenti costituirebbe reato. La tesi della natura bilaterale è prevalsa.

---

<sup>183</sup> Art. 8 del Testo Unico sulla Rappresentanza del 10 gennaio 2014.

<sup>184</sup> L'art. 7 del Testo Unico sulla Rappresentanza del 10 gennaio 2014 riporta che *“le decisioni relative a materie di competenza delle R.S.U. sono assunte dalle stesse, a maggioranza, in base a quanto previsto nella parte terza del presente accordo che recepisce i contenuti dell'accordo interconfederale 28 giugno 2011. Le R.S.U. costituite nelle unità produttive di imprese plurilocalizzate potranno dare vita ad organi o a procedure di coordinamento fissandone espressamente poteri e competenze”*.

<sup>185</sup> ALVINO I., *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*, in *Labour Law Issues*, vol. n. 2, 2016, pp. 19 ss.

È opportuno a tal fine richiamare la Risposta a Interpello del 5 dicembre 2005, con la quale il Ministero del lavoro ha affermato essere sufficiente, per la legittimità dell'accordo, la sua sottoscrizione da parte della sola maggioranza delle R.S.A. o meglio, da parte delle R.S.A. che esprimano la maggioranza del personale, ossia dei lavoratori sindacalizzati dell'unità produttiva, senza che sia necessario il consenso unanime di tutte le R.S.A.<sup>186</sup>. Soluzione che, a ben guardare, non impedisce la stipulazione di un accordo con un'unica R.S.A. qualora sia la sola presente.

L'interpello aveva per oggetto l'istanza avanzata dalla Associazione Bancaria Italiana (ABI) in materia di controlli a distanza e accordi contrattuali. L'ABI richiedeva chiarimenti in merito alla corretta interpretazione dell'art. 4 della L. n. 300/1970, con riferimento a due aspetti.

Il primo ineriva all'individuazione dei requisiti dell'accordo da stipularsi con le R.S.A. legittimante l'installazione di impianti e apparecchiature di controllo a distanza dei lavoratori. Si chiedeva se tale accordo avesse bisogno del consenso unanime di tutte le R.S.A. ovvero ritenesse soddisfacente la sottoscrizione da parte della sola maggioranza delle rappresentanze sindacali aziendali o meglio, da parte delle R.S.A. espressione della maggioranza del personale.

La dottrina era spaccata in due, oscillando tra chi sosteneva la tesi del necessario consenso unanime e chi assecondava quella opposta.

Dal punto di vista giurisprudenziale non può non menzionarsi la decisione della Pretura di Milano, (Ufficio del GIP, 23 luglio 1991) che ha ritenuto legittimo il comportamento del datore di lavoro, che ha proceduto all'installazione di alcune telecamere per la vigilanza di uno sportello bancario automatico previo accordo con la sola maggioranza delle RSA, non essendo integrati gli estremi del reato *ex art. 4, comma 2, St. lav. in combinato disposto con l'art. 38 St. lav. non emendati*, perché destinata l'installazione degli strumenti a garantire la sicurezza di clienti.

È a tale ultimo orientamento che il Ministero del lavoro ha dato seguito in ragione del fatto che, *“la necessaria adesione di tutte le RSA finirebbe per tradursi in un vero e proprio “diritto di veto” utilizzabile anche dalla rappresentanza sindacale più esigua che potrebbe, in tal modo, vanificare l'accordo raggiunto con le altre componenti aziendali”*<sup>187</sup>.

Il secondo chiarimento richiesto riguardava la possibilità di centralizzare la procedura in questione nel luogo ove era ubicata la direzione generale dell'istituto bancario, senza coinvolgere

---

<sup>186</sup> Cfr. BELLAVISTA A., *Gli accordi sindacali in materia di controlli a distanza sui lavoratori*, in *Lav. giur.*, 2014, pp. 737 ss.; ZOLI C., *Il controllo a distanza del datore di lavoro: l'art. 4 l. n. 300/1970 tra attualità ed esigenze di riforma*, in *Riv. dir. it. lav.*, 2009, I, pp. 485 ss.

<sup>187</sup> Interpello 5 dicembre 2005, prot. n. 2975 – Controlli a distanza, di cui all'art. 4 L. n. 300/1970 – Associazione Bancaria Italiana (ABI), su [www.agens.it](http://www.agens.it); Tuttavia, non mancano opinioni dottrinali e giurisprudenziali che sostengono il consenso unanime: in particolare, cfr. ROMAGNOLI U., *Sub art. 4*, in GHEZZI G.- MANCINI G.F., MONTUSCHI L.- ROMAGNOLI U., *Statuto dei diritti dei lavoratori*, Bologna, 1972; CAUTADELLA A., *Dignità e riservatezza del lavoratore (tutela della)*, in *Enciclopedia giuridica Treccani*, XI, 1989, p. 4.

necessariamente le R.S.A. o le D.P.L. delle province dove si trovavano le singole unità produttive dello stesso istituto bancario. In merito, il Ministero precisava che *“in ordine al secondo quesito si ritiene invece che l'accordo raggiunto con le RSA ove è ubicata la direzione generale dell'istituto bancario non sia sufficiente a legittimare l'installazione delle apparecchiature di controllo anche qualora l'impianto tecnologico presenti caratteristiche costruttive e di funzionamento standardizzate e del tutto identiche su tutto il territorio nazionale”*: la ragione di ciò risiedeva nel fatto che, secondo il Ministero, il coinvolgimento delle R.S.A. “più vicine” sarebbe stato giustificato in virtù della natura dei diritti coinvolti, assolutamente personali, come il diritto alla riservatezza del lavoratore<sup>188</sup>. Dunque, l'interpretazione più rigida del necessario consenso unanime di tutte le R.S.A. presenti nell'unità produttiva sembrava da scartare perché, al di là dell'assenza di qualunque indicazione in tal senso nella legge, ciò avrebbe riconosciuto una sorte di potere di veto di una singola R.S.A., anche minoritaria, apparentemente non in linea con la *ratio* della normativa in esame.

Data la sostanziale coincidenza della formulazione nuova con quella del previgente art. 4 St. lav. sul punto si può ritenere che il parere espresso dal Ministero conservi validità anche successivamente alla riforma, intervenuta a distanza di dieci anni dal predetto Interpello.

Pur confermando l'impostazione tradizionale, la nuova disposizione introduce una regola specifica per il caso in cui un'impresa, dotata di unità produttive site in diverse province della stessa regione o in più regioni, sia desiderosa di installare uno stesso strumento di controllo nelle varie unità.

La Suprema Corte, sotto il vigore del vecchio testo, aveva escluso la validità degli accordi collettivi sottoscritti con organi di coordinamento delle R.S.A., precisando la tassatività dell'individuazione dei soggetti abilitati dall'art. 4 St. lav. a concedere l'autorizzazione e la necessità della stipula di un autonomo accordo sindacale in ciascuna unità produttiva per una legittima installazione di apparecchiature<sup>189</sup>. In merito a ciò, l'effetto semplificativo della riforma è stato quello di autorizzare un'impresa plurilocalizzata a concludere per l'installazione di strumenti di controllo, non tanti accordi quante sono le unità produttive in cui si articola, bensì un solo accordo con le associazioni sindacali comparativamente più rappresentative sul piano nazionale.

---

<sup>188</sup> Affermando ciò, è fatto proprio dal Ministero l'orientamento espresso dalla Corte Suprema nella sent. del 16 settembre 1997 n.9211, nella quale si legge che la tassatività dei soggetti indicati dall'art. 4, comma 2, esclude che possa considerarsi il raggiungimento dell'intesa tra datore di lavoro e organi di coordinamento delle R.S.A. di varie unità produttive legittimante l'installazione di strumenti da cui possa derivare un controllo a distanza sull'attività lavorativa, come nella fattispecie, impianti audiovisivi.

<sup>189</sup> Cass., 16 settembre 1997, n.9211, in MGL, 1997, 804.

Vi è poi il bisogno che il contratto collettivo stipulato da tali soggetti qualificati sia espressione della loro maggioranza. Si possono a tal proposito richiamare i criteri desumibili dal Testo Unico del 2014, ovverosia la media del 5% fra dato elettorale e dato elettivo per individuare il sindacato comparativamente più rappresentativo e la percentuale del 50% più uno in relazione a tali sindacati firmatari del contratto collettivo da poter ritenere valido per acquisire da parte del datore di lavoro il consenso a installare impianti audiovisivi e altri strumenti di controllo<sup>190</sup>.

Oltretutto sarebbe stato irragionevole imporre la moltiplicazione degli accordi per ogni unità produttiva, per di più con la possibilità di esiti diversificati, avendo ciascuna R.S.A./R.S.U., per l'unità produttiva dove è costituita, la facoltà di negare il consenso all'accordo che, avrebbe invece potuto essere raggiunto in altre unità produttive.

È infine opportuno segnalare come la trattativa con le associazioni sindacali esterne, anziché con R.S.A./R.S.U., non rappresenti un'attribuzione di competenza esclusiva a tali associazioni, sottratta alle rappresentanze sindacali costituite in azienda, bensì sia un'alternativa facoltativa. E l'esercizio di tale facoltà avverrà in seguito alla valutazione dell'impresa interessata cui spetta l'iniziativa di avviare la trattativa, senza dover necessariamente ottenere il consenso del soggetto sindacale escluso dalla trattativa. Si viene così a tracciare un modello di competenza sindacale concorrente e multilivello<sup>191</sup>.

### **2.3 Il comma 2: le nuove categorie di strumenti**

Se l'autorizzazione sindacale o ministeriale costituisce, anche dopo la riforma, con le ricordate novità, una condizione per l'installazione degli strumenti idonei a realizzare un controllo preterintenzionale, al tempo stesso il nuovo secondo comma dell'art. 4 St. lav. restringe il bacino di dispositivi inclusi in tale categoria.

Esclude infatti l'operatività della disposizione di cui al comma 1 per quegli strumenti utilizzati dal lavoratore *“per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze”*.

Questa disposizione ha provocato invece *“un arretramento della centralità della tradizionale procedimentalizzazione sindacale (o amministrativa) dei poteri datoriali”*<sup>192</sup>, in quanto per installare gli “strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa” e quelli “di

---

<sup>190</sup> PASSALACQUA P., *Il modello del sindacato comparativamente più rappresentativo nell'evoluzione delle relazioni sindacali*, in Dir. rel. ind., 2014, pp. 375 ss.

<sup>191</sup> MARESCA A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.* in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017.

<sup>192</sup> MARAZZA M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in CSDLE “Massimo D'Antona”, n. 300, 2016, p. 15.

registrazione degli accessi e delle presenze” non è più necessario concludere un accordo con il sindacato o ottenere l’autorizzazione in sede amministrativa.

L’entità di tale arretramento dipende dall’ampiezza dell’interpretazione delle nozioni di “strumenti utilizzati per rendere la prestazione lavorativa” e di quelli di “registrazione degli accessi e delle presenze”, nozioni che ora si procederà a ricostruire.

Partendo dalla prima espressione, come accennato nel capitolo precedente, sotto il vigore dell’originario art. 4 St. lav., per quanto una parte della dottrina avesse sostenuto la tesi della esclusione degli strumenti di lavoro dal raggio di quelli soggetti alla procedura di cui al comma 2, l’opinione maggioritaria, condivisa dalla giurisprudenza, era nel senso che anche gli strumenti potenzialmente di lavoro, insieme alle apparecchiature di rilevazione degli accessi, dovessero essere impiegati previo ottenimento dell’autorizzazione. Tale impostazione aveva generato problemi applicativi, inducendo le imprese a installare le apparecchiature in questione senza cercare di ottenere la preventiva autorizzazione sindacale o ministeriale; imprese che, bisognose di installare strumenti, perché essenziali al compimento della prestazione dovuta dal dipendente, preferivano agire senza essere in regola con la disposizione, per non incappare nelle conseguenze di un eventuale mancato accordo sindacale, di un diniego di autorizzazione o, al contrario, di un suo ottenimento comportante limiti eccessivi all’uso dello strumento<sup>193</sup>.

La decisione del Legislatore, presa per il nuovo art. 4 St. lav., di estromettere esplicitamente l’installazione degli strumenti menzionati dal regime autorizzatorio appare una notevole semplificazione, utile a evitare ritardi e inefficienze connaturate a tale impianto sistematico in relazione a quelle apparecchiature utilizzabili per l’esecuzione della prestazione. Si supera così quell’obsolescenza tecnica contestata al vecchio art. 4 St. lav., in quanto gli strumenti a cui qui il Legislatore fa riferimento sono evidentemente quelli tipicamente informatici, quali computer, tablet, telefonino ecc.

Al tempo stesso ciò non deve indurre a pensare che tale esclusione abbia dato al datore di lavoro il via libera per monitorare costantemente l’attività del lavoratore tramite l’analisi dei dati registrati dallo strumento di lavoro. La possibilità di installare quest’ultimo va tenuta separata da quella di esaminare le informazioni ottenute con il suo utilizzo e in seguito immagazzinate: al datore infatti non è accordato il libero esame dei dati ricavati dall’uso di strumenti di lavoro, essendo piuttosto tenuto al rispetto dei limiti posti dall’ordinamento a tutela della dignità e riservatezza del lavoratore, così come delineati dal terzo comma dell’art. 4 St. lav., su cui ci soffermeremo più avanti.

---

<sup>193</sup> ALVINO I., *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*, in *Labour Law Issues*, vol. n. 2, 2016.

Il fatto che non sia riportato l'inciso del primo comma "dai quali possa derivare un controllo a distanza" accentua il problema e l'esigenza di identificare gli strumenti che possano ricadere nell'eccezione del comma 2 piuttosto che nella regola di carattere generale del comma 1.

Facendo leva sul fatto che la riconducibilità degli strumenti in uno dei primi due commi dell'art. 4 St. lav. debba avvenire e, in base all'hardware, e, in base al software<sup>194</sup>, si può affermare che gli strumenti di cui si discute non siano gli strumenti di lavoro tradizionali, nel senso di attrezzi o dotazioni individuali di ciascun dipendente, bensì sono quelli che spesso coincidono con il sistema informatico di cui si è dotata l'impresa centralmente e al quale si connettono i lavoratori, utilizzando postazioni fisse o mobili, per eseguire le attività di lavoro<sup>195</sup>.

È poi puntualizzato che gli strumenti di cui si tratta devono essere "*strumenti utilizzati per rendere la prestazione*". Essa è espressione più circoscritta rispetto a quella di "*strumenti di lavoro*", menzionata dalla legge delega 183/2014, nel senso che non tutte le funzioni di un medesimo strumento informatico di lavoro, ad es., computer, notebook, smartphone, ecc., rientrano nel campo di applicazione del secondo comma, ma soltanto quelle funzioni (programmi, software o applicazioni) che appunto sono utilizzate per rendere la prestazione lavorativa (ad esempio, i programmi di scrittura, di calcolo, di elaborazione delle immagini o di progetti, come word, power point, excel, photoshop; i programmi di navigazione nelle rete internet e di gestione della posta elettronica aziendale, ecc.); non vi rientrano funzioni e relativi programmi non costituenti strumento di esecuzione della prestazione, installati e utilizzati prevalentemente ad altri fini, anche se accessori o connessi alla prestazione stessa (ad esempio, di sicurezza, come i programmi antivirus,

---

<sup>194</sup> MARRAZZA M. *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in WP C.S.D.L.E. "Massimo D'Antona". IT – 300/2016 sottolinea che producendo gli applicativi informatici di ciascuna rete digitale informazioni che il datore registra, i cd. *log*, si prestano a essere qualificati sia come strumento di controllo, se il dipendente è soggetto passivo del controllo che essi permettono, che come strumento di lavoro, se invece il lavoratore li utilizza attivamente nell'esecuzione della prestazione. Se il software è in grado di produrre log, ossia di tracciare l'attività del dipendente, di per sé, nel senso che questa è una funzione che si atteggia a una caratteristica intrinseca del software stesso, e non l'effetto tecnico di un applicativo aggiuntivo, esso è qualificabile come strumento di lavoro e ricade nell'area dell'art. 4, comma 2, St. lav., ond'è che il successivo utilizzo dei dati tracciati tramite esso è ammesso nel rispetto di quanto dettato all'art. 4, comma 3, St. lav. Se lo stesso software invece necessita, per la produzione di log, dell'installazione di un altro applicativo, il primo è uno strumento di lavoro ma il controllo effettuato tramite il secondo richiede l'autorizzazione di cui all'art. 4, comma 1, St. lav., per quanto i due software siano installati sullo stesso hardware. Si tratta ovviamente di un approccio qualificatorio che postula accertamenti tecnici sulle funzionalità del software preso in considerazione. In senso contrario MAIO V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in Arg. Dir. Lav., 2015, p.6, che sostiene la nozione unitaria e più ampia di strumento di lavoro che finisce per ricomprendere, senza distinzioni, tutte le funzionalità disponibili sul medesimo apparato hardware.

<sup>195</sup> MARESCA A. op. cit.

o quelli di localizzazione satellitare). Questi ultimi confluiscono piuttosto nel campo di applicazione del comma 1 dell'art. 4 St. lav.<sup>196</sup>

È vero che si potrebbe obiettare che gli strumenti cui si riferisce l'espressione in esame potrebbero essere non solo quelli necessari a espletare il proprio lavoro, ma anche quelli che ne agevolano lo svolgimento, facendo leva sul fatto che l'art. 4, comma 2, St. lav. non parla di strumenti "necessari", ma di quelli "utilizzati" per rendere la prestazione.

In tal modo, tuttavia, per installare larga parte degli strumenti dai quali può derivare un controllo sull'attività dei lavoratori non sarebbe indispensabile un accordo con il sindacato o un'autorizzazione amministrativa e sarebbe difficile affermare, come si è fatto sopra, che il novellato art. 4 abbia mantenuto la storica centralità del procedimento di controllo sindacale o amministrativo. Se, ciò nonostante, si considera che, anche a seguito delle modifiche da ultimo apportate, l'art. 4 St. lav. non è volto a dare assoluta preminenza alle esigenze di controllo del datore di lavoro, ma a bilanciare la dignità e riservatezza dei lavoratori con gli interessi dell'impresa e che la procedimentalizzazione dei poteri datoriali è finalizzata proprio a consentire un miglior contemperamento degli interessi contrapposti delle parti, gli "strumenti utilizzati per rendere la prestazione" possono essere intesi in senso restrittivo come quelli necessari a svolgere le mansioni assegnate al lavoratore, da lui impiegati direttamente a tale scopo e il cui funzionamento richiede una partecipazione attiva del lavoratore.

In tal modo si riduce la platea di apparecchiature la cui installazione è sottratta alla procedura sindacale o amministrativa.

In questa direzione, con il suo comunicato stampa del 18 giugno del 2015 il Ministero del lavoro ha specificato che "*non possono essere considerati "strumenti di controllo a distanza" gli strumenti che vengono assegnati al lavoratore "per rendere la prestazione lavorativa"*", ossia quei mezzi che "servono" al lavoratore per adempiere la prestazione, precisando poi che se lo strumento in questione subisce modifiche volte a controllare il lavoratore stesso, l'eccezione del comma 2 non trova applicazione e, pertanto, ai fini dell'installazione, sono necessari sia il rispetto della procedura autorizzatoria, sia le esigenze organizzative e produttive, per la sicurezza del lavoro e la tutela del patrimonio. A titolo esemplificativo, il datore di lavoro non dovrà ottenere l'autorizzazione in sede sindacale o amministrativa per installare un software sui computer aziendali solo se quest'ultimo è necessario per svolgere la prestazione lavorativa. Se, al contrario, non è necessario perché la

---

<sup>196</sup> Questo è chiarito anche dal Comunicato stampa del Ministero del lavoro del 18 giugno 2015, "Controlli a distanza: Ministero del lavoro, nessuna liberalizzazione; norma in linea con le indicazioni del Garante della Privacy", su <https://www.lavoro.gov.it/>.

prestazione sia utile al datore di lavoro, il software potrà essere installato solo dopo aver raggiunto l'accordo in sede sindacale o dopo aver ottenuto l'autorizzazione amministrativa<sup>197</sup>.

In linea con ciò, l'Ispettorato nazionale del lavoro, con circolare n. 2 del 7 novembre 2016, ha precisato che possono considerarsi strumenti di lavoro “*gli apparecchi, dispositivi, apparati e congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità siano stati posti in uso e messi a sua disposizione*”. Gli strumenti, presi in considerazione dal comma 2, sono dunque quelli “*strettamente e direttamente funzionali all'adempimento degli obblighi lavorativi ed implicanti una partecipazione attiva del lavoratore*”<sup>198</sup>, con conseguente esclusione delle strumentazioni estranee alla mansione: la mancanza di tale stretta funzionalità porterebbe a ricadere nell'alveo del comma 1 dell'art. 4 St. lav<sup>199</sup>.

Analogamente, con verifica preliminare del 16 marzo 2017 il Garante privacy, concorde con l'Ispettorato, ha confermato che gli strumenti di lavoro sono tutti quei dispositivi “*utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa*”, ovvero sia “*direttamente preordinati all'esecuzione della prestazione lavorativa*”. Si tratta dunque di dispositivi dotati di un nesso di strumentalità diretta con l'effettuazione della prestazione da parte del lavoratore, mezzi funzionali alla corretta esecuzione della mansione oggetto del contratto di lavoro, che permettano al dipendente di adempiere la sua principale obbligazione di rendere la prestazione in modo che sia utile al datore secondo l'organizzazione procedurale predisposta dall'imprenditore stesso<sup>200</sup>.

Dalla definizione di strumento di lavoro elaborata, sia l'INL che il Garante della privacy hanno desunto che i sistemi di geo-localizzazione (es. i satellitari GPS montati su auto aziendali), che verranno approfonditi in seguito, rappresentano un elemento “aggiunto” agli strumenti di lavoro in quanto non utilizzati in via primaria per l'esecuzione dell'attività lavorativa. Ne consegue che, in tali casi, si applicherebbe il comma 1 dell'art. 4 St. lav.

Nei provvedimenti citati, tuttavia, l'INL e il Garante individuano dei casi particolari in cui si può ritenere che i GPS siano veri e propri strumenti di lavoro<sup>201</sup>.

---

<sup>197</sup> Cfr. VILLA E., *Accordo sindacale e procedura amministrativa nei controlli a distanza dei lavoratori*, su <http://www.dirittolavorovariazioni.com/>; CAIRO L., *Semplificazione delle procedure e controlli a distanza*, Milanofiori Assago (MI), 2016.

<sup>198</sup> CIARAFONI A., *I controlli dei lavoratori nel contesto tecnologico: un difficile tentativo di bilanciamento d'interessi contrastanti*, su <https://www.iusinitinere.it/>.

<sup>199</sup> Cfr. DEL PUNTA R., *La nuova disciplina dei controlli a distanza sul lavoro*, in Riv. It. Dir. Lav., 2016, I, p. 99; DE LUCA TAMAJO R. - MAZZOTTA O., *Commentario breve alle leggi sul lavoro*, Milanofiori Assago (MI), 2018.

<sup>200</sup> In questo senso anche la Circolare n. 20/2015 della Fondazione Studi dei Consulenti del Lavoro.

<sup>201</sup> Si tratta del caso in cui i sistemi di localizzazione siano installati per consentire la concreta ed effettiva attuazione della prestazione lavorativa (cioè la stessa non possa essere resa senza ricorrere all'uso di tali strumenti), ovvero del caso in cui l'installazione sia richiesta da specifiche normative di carattere legislativo o regolamentare (es. uso dei sistemi GPS per il trasporto di portavalori superiore a euro 1.500.000,00).

Questo prova dunque come l'intervento del Garante non sia risolutivo rispetto alle problematiche evidenziate, essendo necessaria una valutazione da effettuarsi caso per caso, in quanto la "stretta funzionalità" di un software e/o di un applicativo rispetto alla prestazione lavorativa (anche in termini di sicurezza) non può prescindere da una verifica della specifica attività svolta dal lavoratore e/o del settore nel quale egli opera.

Altra categoria problematica e di cui si è occupato l'INL (circolare n. 4 del 26 luglio 2017) è costituita dai sistemi di gestione dell'anagrafica del cliente e dei dati relativi ai rapporti contrattuali in essere con il gestore telefonico che rendono più completa l'informazione e più efficiente la relazione tra il chiamante e l'operatore.

Si tratta di archivi informatici che sostituiscono il fascicolo cartaceo del cliente e consentono di avere a disposizione tutti i dati necessari a evadere le richieste avanzate da questi, gestione che sarebbe più difficoltosa in caso di ricerca manuale dei dati dello stesso. Software del genere, che permettono il mero accoppiamento fra la chiamata e l'anagrafica del cliente senza possibili ulteriori elaborazioni, possono essere considerati uno strumento utile al lavoratore per rendere la prestazione lavorativa. Accanto a tali sistemi sono individuabili ulteriori software che, invece, raccolgono ed elaborano in tempo reale i dati relativi agli stati di attività telefonica di ciascun operatore (libero, non disponibile, in pausa) e i tempi medi di evasione delle diverse lavorazioni, che quantificano la produttività giornaliera per ogni servizio reso, il tempo dedicato al lavoro per ciascuna commessa e le pause effettuate da ogni singolo lavoratore. Questi sistemi, funzionali a più o meno generiche esigenze produttive e lungi dall'essere indispensabili per lo svolgimento della prestazione, consentono di realizzare un monitoraggio costante su tutti gli operatori e, pertanto, rientrano nel campo applicativo dell'art. 4, comma 1, St. lav. Tale distinzione è stata ribadita anche dal Garante privacy con provvedimento n. 139 dell' 8 marzo 2018<sup>202</sup>, secondo cui il sistema che gestisce le chiamate di un call center dedicato agli abbonati di un dato servizio e che non si limiti ad associare la chiamata e l'anagrafica del cliente per facilitare la gestione della richiesta dell'abbonato, ma consenta ulteriori elaborazioni (es. memorizzazioni di dati personali degli operatori ed estrazione di report), non può essere considerato uno strumento di lavoro utilizzato dall'operatore per rendere la prestazione; esso rientra tra gli strumenti diretti a soddisfare esigenze organizzative e produttive del datore di lavoro dai quali può derivare il controllo a distanza dei lavoratori<sup>203</sup>.

---

<sup>202</sup> Con segnalazione una organizzazione sindacale e alcuni operatori di customer care in servizio presso Sky Italia Network Service S.r.l. hanno lamentato la possibile violazione della disciplina in materia di protezione dei dati personali per effetto dell'impiego da parte della società del software gestionale "Salesforce Arcadia" introdotto nell'Unità produttiva presso la sede di Milano e quella di Sestu (Cagliari), senza fornire una preventiva ed esaustiva informativa ai dipendenti.

<sup>203</sup> CAZZELLA A., *La definizione di "strumento di lavoro" ex art. 4 Stat. Lav. secondo il Garante della privacy*, su <http://www.diritto24.ilsole24ore.com/>.

Alla luce di tali considerazioni, sembra perciò attualissimo quanto dettato dalla sentenza del Pretore di Milano del 5 dicembre 1984 nella quale si legge che in definitiva *“il problema è quello di definire se la capacità di uno strumento di lavoro di lasciare e registrare traccia del proprio utilizzo possa far trasmodare l'apparecchio, limitatamente a tale aspetto, da strumento di lavoro a strumento di controllo del lavoratore”*<sup>204</sup>.

Altro profilo d'indagine è quello che riguarda gli strumenti di lavoro che il dipendente è autorizzato a utilizzare anche nella propria sfera strettamente privata, come il telefono per uso promiscuo, e cioè, per ragioni del tutto estranee alla sfera dell'adempimento della prestazione di lavoro.

In tale ipotesi appare evidente che lo strumento legittimamente usato per esigenze extra lavorative non può consentire un tracciamento di dati, né la loro utilizzabilità ai fini connessi al rapporto di lavoro. Si tratterà piuttosto di individuare protocolli tecnologici in grado di rilevare la distinzione della sfera personale e professionale di impiego di un certo strumento, o di precluderne l'utilizzo privato.

La nuova norma non richiede più alcuna autorizzazione preventiva nemmeno per installare e utilizzare gli strumenti di rilevazione degli accessi e delle presenze<sup>205</sup>, in quanto si tratta di strumenti finalizzati a fornire al datore di lavoro informazioni sull'ora di entrata e di uscita dal luogo di lavoro, appurando così il rispetto dell'orario di lavoro, ma astenendosi dal rivelare informazioni sul contenuto dell'attività svolta. Non risultano dunque in pericolo i beni protetti dalla disposizione in commento, dignità e riservatezza, a fronte di un eventuale utilizzo dei predetti strumenti.

Il Legislatore prende in tal modo posizione rispetto a un orientamento giurisprudenziale, non univoco ma ampiamente condiviso dalla Suprema Corte<sup>206</sup>, che affermava l'applicabilità del vecchio comma 2 dell'art. 4 St. lav. al sistema informatizzato di rilevazione delle presenze all'inizio e alla fine dell'orario di lavoro, in quanto atto a realizzare un controllo a distanza sui tempi della prestazione dovuta dal lavoratore, con la conseguenza che l'attivazione di tale sistema avrebbe dovuto essere preceduta dall'accordo sindacale o dell'autorizzazione amministrativa.

---

<sup>204</sup> Pret. Milano, 5 dicembre 1984, in Foro it., 1985, p. 285.

<sup>205</sup> Sono strumenti funzionali ad accertare la presenza le tessere elettroniche o badge, i sistemi di rilevazione antropobiometrici, ossia sistemi che rilevano l'identità del lavoratore tramite corrispondenza delle impronte digitali o palmari o dell'iride con i dati personali già memorizzati, o i microchip sottocutanei. Di questi ultimi, pur rientrando in tale categoria, non si hanno notizie del loro uso in Italia: per combattere l'assenteismo interno e la scarsa produttività, da gennaio 2015 l'Epicenter, questo il nome dell'azienda promotrice dell'esperimento che opera nel campo dell'hi-tech, con sede a Stoccolma e circa 700 dipendenti, ha dato il via ad una piccola rivoluzione, innestando un microchip sottopelle a tutti i suoi dipendenti che l'hanno accettato. Sul punto PEROSINO M., *Un chip sottopelle come nei film: ecco la mia nuova vita da cyborg*, su <https://www.lastampa.it/>.

<sup>206</sup> Cfr., sul punto, Cass. 17 luglio 2007, n. 15892, in Riv. it. dir. lav., 2008, II, 714.

Maggiori dubbi possono sorgere in relazione all'utilizzo di strumenti che registrano l'entrata dei lavoratori in specifici luoghi aziendali, come il passaggio da un reparto all'altro, permettendo al datore di lavoro di ricostruire minuziosamente gli spostamenti del lavoratore all'interno del luogo di lavoro.

Gli strumenti che rilevano gli accessi consentono, di regola, di sapere chi è presente sul luogo di lavoro, piuttosto che di registrare l'inizio e la fine dell'attività lavorativa.

La congiunzione “e” collocata fra i termini “accessi” e “presenze” assumerebbe un valore disgiuntivo, atto a esprimere che il concetto di “accesso” ha un suo significato autonomo da quello di “presenza”. Lo strumento al quale la disposizione fa riferimento non è dunque solo quello che permette di rilevare gli accessi del lavoratore sul luogo di lavoro, solo per una rilevazione della presenza e dunque del rispetto dell'orario di lavoro, ma qualunque strumento idoneo a registrare l'accesso e/o la presenza in determinati locali aziendali. L'apparecchiatura destinata a rilevare l'accesso e la presenza (e quindi i tempi e la durata della presenza, nonché il transito da un luogo ad un altro) può allora essere liberamente installata dal datore di lavoro nei locali aziendali nei quali la ritenga necessaria, avendo ricevuto in tal senso una autorizzazione ampia e generale dallo stesso art. 4<sup>207</sup>.

Alla luce di tali riflessioni si può concludere che l'introduzione del secondo comma significa non solo che rispetto ai controlli resi possibili dalle apparecchiature esaminate non operano gli oneri procedurali esaminati, ma anche e soprattutto che tramite esse si potrà effettuare un controllo a prescindere dalle finalità sopra richiamate: pertanto il datore di lavoro può svolgere i controlli funzionali all'accertamento di inadempimenti contrattuali e illeciti extra-contrattuali, fermi restando i limiti della rilevanza ai fini della valutazione dell'attitudine professionale (art. 8 St. lav.) del rispetto della dignità del lavoratore, della riservatezza sua e di terzi, e del rispetto della tutela generale civilistica in materia di privacy.

E a ben guardare sotto questo aspetto l'esito della riforma potrebbe apparire non del tutto rispettoso delle finalità di protezione che il Legislatore avrebbe dovuto prefiggersi di perseguire; ogni strumento di lavoro informatico/tecnologico è infatti generalmente dotato di una notevole capacità di immagazzinare (tramite i cd. “*file log*” che, conservati con una periodicità regolare, diventano disponibili a supporto delle attività di monitoraggio, o di *logging*, e di amministrazione funzionale) dati relativi alla sequenza anche cronologica delle operazioni compiute dal lavoratore, man mano che queste vengono eseguite dal sistema o dall'applicazione, rendendo possibile un monitoraggio

---

<sup>207</sup> ALVINO I. op. cit.

piuttosto incisivo. Il venir meno di qualunque cautela nei confronti degli strumenti di lavoro potrebbe portare a un approccio “disinibito” agli stessi<sup>208</sup>.

Tale lettura porta inevitabilmente a condividere l’opinione espressa dal Garante privacy nell’intervento del 13 gennaio 2015, secondo cui l’unico limite al controllo sui lavoratori, con riferimento agli strumenti utilizzati da questi per render la prestazione è rappresentato dal Codice della privacy, il che significa che “*i controlli datoriali devono comunque essere improntati a gradualità nell’ampiezza e nella tipologia con assoluta residualità dei controlli più invasivi, legittimati solo a fronte di specifiche anomalie e comunque all’esito dell’esperimento di misure preventive meno limitative dei diritti dei lavoratori*”<sup>209</sup>.

### **3. L’utilizzabilità dei dati raccolti e la tutela della riservatezza del lavoratore**

Si può ora passare all’analisi del secondo nucleo normativo contenuto nell’art. 4, comma 3, St. lav. Ricostruite infatti le regole che governano l’installazione dello strumento dal quale può discendere la possibilità di sorvegliare a distanza l’attività lavorativa, occorre esaminare il momento logicamente successivo: quello dei limiti entro i quali i dati raccolti dall’apparecchiatura possano essere usati dal datore di lavoro.

Con quest’ultima disposizione il Legislatore ha aggiornato la disciplina del potere di controllo, regolamentando tutte le fasi della relativa attività di controllo in vista del soddisfacimento del bisogno di protezione della dignità e della riservatezza del lavoratore.

#### **3.1 La regola generale dell’utilizzabilità e l’informazione al lavoratore**

Prescrivendo il nuovo comma 3 che “*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*”, è cristallino riguarda una fase che si colloca a valle del controllo, quando questo si è ormai esaurito, essendo le informazioni entrate nella disponibilità del datore di lavoro, il quale potrà sfruttarle a distanza di tempo o luogo dal momento della loro acquisizione.

Tale profilo, di regolamentazione dell’istante di rilevazione e acquisizione dell’informazione e del trattamento del dato registrato da parte del datore di lavoro, non trovava un suo disciplinamento all’interno del testo originario dell’art. 4 St. lav., limitandosi quest’ultimo a dettare solo le

---

<sup>208</sup> SITZIA A., *Il controllo (del datore di lavoro) sull’attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore)*, vol. 2, no. 1, 2016.

<sup>209</sup> SORO A., *I lavoratori devono essere informati. Il datore di lavoro non può spiare le mail*, ne L’Huffington post, 13 gennaio 2016; sul punto anche Cass., 14 luglio 2017, n. 17531, su <https://www.studiocerbone.com/>.

condizioni da rispettare per la legittima installazione dell'apparecchiatura, ovvero per la "predisposizione del controllo"<sup>210</sup>. E tale lacuna, in quanto fonte di incertezze applicative in ordine all'uso delle informazioni raccolte mediante il controllo a distanza, è stata una delle cause primarie di inefficienza della vecchia regola.

Il silenzio mantenuto su tale aspetto dall'art. 4 St. lav. innescava varie conseguenze.

In primo luogo, da un lato portava a ritenere connessa alla legittimità del controllo a distanza la facoltà del datore di lavoro di avvalersi dei dati registrati, dal lato opposto, che il limite stabilito dal legislatore del 1970 ai controlli a distanza, in funzione di esigenze organizzative e produttive o dettate dalla sicurezza del lavoro, operasse pure con riferimento all'impiego dei dati acquisiti.

In secondo luogo risultava rimesso alla giurisprudenza il compito di verificare la legittimità delle azioni e delle sanzioni promosse contro il lavoratore<sup>211</sup>: sotto il vigore della vecchia norma, la giurisprudenza si era pronunciata sovente sulla legittimità dei controlli sui lavoratori, eppure la dottrina aveva evidenziato come, nella maggior parte di queste pronunce, il rispetto dei principi fondamentali del trattamento dei dati, nelle modalità concrete con cui il controllo si svolgeva in azienda, fosse valutato raramente<sup>212</sup>.

La questione è oggi risolta grazie al comma 3 dell'art. 4 St. lav. che incide sulla posizione del datore di lavoro ogni qual volta intenda avvalersi dei dati raccolti. Decisione subordinata alle condizioni indicate dal Legislatore che tracciano il *discrimen* tra uso legittimo e illegittimo dei dati stessi.

Il Ministero del lavoro, infatti, nella nota del 18 giugno 2015, espone la *ratio* del nuovo art. 4, comma 3, St. lav. illustrando che: *"La norma non "liberalizza" i controlli ma si limita a fare chiarezza circa il concetto di "strumenti di controllo a distanza" ed i limiti di utilizzabilità dei dati raccolti attraverso questi strumenti, in linea con le indicazioni che il Garante della Privacy ha fornito negli ultimi anni e, in particolare, con le linee guida del 2007 sull'utilizzo della posta*

---

<sup>210</sup> CONTE D., *Riflessioni sull'articolo 4 dello statuto dei lavoratori alla luce della consistenza trifasica del controllo*, in *Lavoro e previdenza oggi*, 1-2, 2017, p. 2, afferma che *"l'attività di controllo passibile di essere ritenuta regolata dall'art. 4, ha una consistenza che si articola in almeno tre "fasi" o "momenti" tra loro distinti (c.d. consistenza "trifasica" del controllo): quella di predisposizione del controllo, che consiste nell'attività di ideazione, progettazione, installazione e programmazione dello strumento destinato al controllo; quella della rilevazione acquisizione in tempo reale dell'informazione da parte dello strumento; quella del trattamento da parte del datore di lavoro o di suoi incaricati del dato registrato"*.

<sup>211</sup> Cfr. BARRACO E. – SITZIA A., *Il problema dei "controlli difensivi" del datore di lavoro: estne saepe ius summus malitia?*, in *Lav. giur.*, 2010, 993; CINQUE G., *Sull'ammissibilità e i limiti dei cd. controlli difensivi del patrimonio aziendale*, in *Orient. Giur. lav.*, 2010, 616; CORDEDDA G., *Controlli a distanza sull'attività dei lavoratori: l'interpretazione dell'art. 4 SL secondo la giurisprudenza recente*, in *D&L-Riv. crit. dir. lav.*, 2007, 1058; FONTANA A., *In tema di "controlli a distanza"*, in *Dir. lav.*, 1985, II, 202; NOGLER L., *Sulle contraddizioni logiche della cassazione in tema di diritto alla riservatezza del lavoratore subordinato*, in *Resp. civ. prev.*, 1998, 111.

<sup>212</sup> AIMO M., *La c.d. cybersurveillance sui luoghi di lavoro*, in TULLINI P. (cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, Padova, 2010.

*elettronica e di internet. (...) Perciò, è bene ribadirlo, non si autorizza nessun controllo a distanza; piuttosto, si chiariscono le modalità per l'utilizzo degli strumenti tecnologici impiegati per la prestazione lavorativa e i limiti di utilizzabilità dei dati raccolti con questi strumenti”.*

Tale comma costituisce dunque il passaggio nevralgico dell'articolo novellato, esprime la nuova filosofia di fondo dell'art. 4 St. lav., un punto di scardinamento tra la vecchia e la nuova normativa statutaria, dettando al contempo alle aziende precise linee guida da seguire per giungere al risultato da sempre bramato.

L'utilizzabilità delle informazioni raccolte tramite l'effettuazione di controlli è legittima a delle condizioni: che avvenga per fini connessi al rapporto di lavoro, che al lavoratore sia preliminarmente fornita un'adeguata informazione sulle modalità d'uso degli strumenti, in particolare quelli tecnologici, nonché sui controlli, e che sia rispettato il Codice della privacy.

Per il trattamento dei dati non è quindi necessario acquisire il consenso del lavoratore, essendo sufficiente l'unilateralità dell'informazione datoriale: il nuovo comma 3 parla espressamente di informazione data al lavoratore e quindi essa è configurata come atto unilaterale del datore che non richiede alcun consenso del dipendente. Tale scelta legislativa di non subordinare al consenso del lavoratore l'utilizzabilità dei dati lecitamente raccolti rappresenta e, un ulteriore punto di discontinuità con la giurisprudenza che, in assenza di una specifica disciplina sul punto, in passato valorizzava anche tale elemento quale forma di tutela dei lavoratori contro “*forme subdole di controllo della loro attività da parte del datore di lavoro*”<sup>213</sup> e, un capovolgimento della tradizionale prospettiva del Codice privacy, che qualificava l'informativa come atto preliminare all'eventuale consenso dell'interessato e non, come invece avviene nella disciplina giuslavoristica, quale condizione di legittimità, in sé considerata, del trattamento<sup>214</sup>. Peculiarità che esclude la necessità di acquisire il consenso del lavoratore e che ben si giustifica se si considera che i dati da

---

<sup>213</sup> Cass., 11 giugno 2012, n. 2261, su <https://www.altalex.com/>. Con tale sentenza la Cassazione penale aveva sostenuto la tesi (improbabile) dell'equipollenza tra consenso individuale dei lavoratori e accordo sindacale. Tale pronuncia, oltre a essere in contrasto con la consolidata giurisprudenza lavoristica in materia, è stata ben presto contraddetta dalla stessa Sezione penale. È stata apertamente contraddetta dalle successive pronunce di Cass. 10 ottobre 2012, n. 16622, in Not. giur. lav., 2012, p. 462, e, in sede penale, Cass., 31 gennaio 2017, n. 22148, in GiustiziaCivile.com, fasc. 7 febbraio 2018, quest'ultima ha evidenziato come la norma penale di cui all'art. 4 St. lav. non si limiti a tutelare la posizione giuridica dei singoli lavoratori bensì è posta a garanzia di “interessi di carattere collettivo e superindividuale”, di cui “le rappresentanze sindacali sono portatrici”. Come affermato dalla più autorevole dottrina, l'indicazione dei soggetti collettivi legittimati a concludere l'accordo sindacale, infatti, deve considerarsi tassativa e, in considerazione della garanzia degli interessi collettivi e superindividuali a cui è preordinato, soltanto l'accordo con le rappresentanze sindacali richiamate dalla legge sarà idoneo al soddisfacimento degli obblighi procedurali, senza possibilità di letture estensive del dettato normativo. Sul punto si veda *ex pluris v. BELLAVISTA A., Gli accordi sindacali in materia di controlli a distanza sui lavoratori*, in Lav. nella giur., 2014, 8-9, p. 738, il quale cataloga la sentenza di Cassazione penale, 11 giugno 2012, n. 22611, alla stregua di un vero e proprio “strafalcione”.

<sup>214</sup> In passato al consenso si riconosceva una maggiore rilevanza: sebbene la disposizione non lo prevedesse, comunque si teneva conto della normativa in materia di privacy che, prescrivendo i casi in cui il consenso non era necessario, all'art. 24 del d.lgs. 196/2003, lo configurava come elemento fondante in tutte le altre ipotesi. L'art. 24 del d.lgs. 196/2003 è stato poi abrogato dal d.lgs. 101/2018.

trattare sono raccolti tramite strumenti di lavoro (art. 4, comma 2, St. lav.), il cui impiego non può dipendere da una manifestazione di volontà del lavoratore o, comunque, mediante strumenti di controllo preventivamente autorizzati dall'accordo collettivo o dal provvedimento amministrativo per finalità legislativamente tipizzate (art. 4, comma 1, St. lav.)<sup>215</sup>.

In epoca antecedente alla riforma si era discusso sul riconoscere o meno al consenso prestato dal lavoratore la forza di consentire i controlli a distanza in deroga all'art. 4 St. lav.: in realtà, l'indisponibilità del diritto tutelato e la scelta in favore di un meccanismo autorizzatorio dei controlli preterintenzionali di matrice sindacale erano già una spia dell'irrilevanza del consenso nell'ambito della norma statutaria.

L'art. 4, comma 3, St. lav., ad oggi, dunque legittima l'utilizzo delle informazioni a condizione che al lavoratore sia stata data "*adeguata informazione*".

L'informativa, quindi, rappresenta la *condicio sine qua non* ai fini della legittimità di qualsivoglia utilizzo delle informazioni raccolte, in quanto la mera sussistenza delle ragioni organizzative e produttive, di sicurezza sul lavoro o tutela del patrimonio aziendale non sono di per sé sufficienti. Queste ultime, difatti, costituiscono una mera precondizione, che deve essere necessariamente accompagnata da un *quid pluris*: l'adeguata informazione.

L'interpretazione dell'inciso normativo per cui il lavoratore deve essere informato adeguatamente sulle modalità di uso degli strumenti e di effettuazione dei controlli, nel rispetto della disciplina in materia di privacy, ha posto il problema di configurare l'attività che il datore di lavoro è chiamato a porre in essere per adempiere a tale obbligo.

Per sciogliere questo nodo si deve partire da un presupposto: la comunicazione deve avvenire personalmente a ogni singolo dipendente. Dal dettato normativo non si ricava alcuna prescrizione circa le modalità e la forma dell'informazione adeguata, ma, in considerazione delle sue finalità, sembra preferibile la redazione di un'informativa a carattere individuale, anziché di tipo collettivo, che dia conto in modo mirato delle attività di controllo a cui è soggetto il singolo lavoratore. Ciascun lavoratore dovrà comprendere attraverso quali strumenti si concreta l'attività di controllo nei suoi confronti e sapere, nel caso questi fossero a lui affidati per l'espletamento delle sue mansioni, come il loro uso si raccordi con l'attività di controllo, quale tipologia di dati sarà trattata e

---

<sup>215</sup> Cfr. MARRAZZA M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in WP C.S.D.L.E. "Massimo D'Antona". IT – 300/2016; MARESCA A., *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore*, in Forum Tuttolavoro (web), 2016; in senso contrario, cioè a favore del necessario consenso del lavoratore, per quanto l'opinione riportata sia quella maggiormente sostenuta, cfr. CARINCI M.T., *Il controllo a distanza dell'attività dei lavoratori dopo il Jobs Act (art. 23 d.lgs. 151/2015): spunti per un dibattito*, in Labour & Law Issues, 2016, vol. 2, n.1; SITZIA A., *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore)*, vol. 2, no. 1, 2016.

quali sono i margini di utilizzabilità. Inoltre, nel silenzio dell'art. 4 St. lav., si ritiene che la comunicazione debba avere la forma scritta, che debba essere preventiva e che, al fine della prova, possa essere opportuna la sottoscrizione per ricevuta da parte del lavoratore. Tale obbligo di comunicazione, di conseguenza, non può essere adempiuto tramite una mera informativa sindacale o attraverso una semplice affissione in bacheca e, inoltre, sembra difficile ipotizzare che possa avvenire tramite e-mail inviata alla casella personale del dipendente, in quanto verrebbe a mancare la prova dell'avvenuta consegna, a meno che non si tratti di una casella di posta elettronica certificata (c.d. PEC).

Rispettate tali condizioni, i dati acquisiti tramite l'uso degli strumenti di controllo a distanza sono impiegabili in sede anche disciplinare.

Al contrario, sotto il vigore del vecchio testo della disposizione in esame, la prova di un eventuale inadempimento contrattuale del lavoratore, frutto di un controllo preterintenzionale o anche difensivo, non poteva mai essere utilizzata in sede disciplinare, come già ricordato. La necessità di tale precisazione nasce dal fatto che, talvolta, si leggeva in giurisprudenza che il controllo preterintenzionale implicava il rispetto dell'art. 4, comma 2, St. lav., con la conseguenza che il mancato esperimento della procedura codeterminativa imponeva la non utilizzabilità in sede disciplinare dei dati acquisiti con il controllo preterintenzionale stesso<sup>216</sup>. In realtà, gli esiti di un controllo preterintenzionale non potevano mai essere utilizzati in sede disciplinare, nemmeno in ossequio alla richiamata procedura da parte del datore di lavoro. Tale limite oggi è destinato a cadere<sup>217</sup>.

Vale la pena notare, a questo punto, che l'utilizzo dei dati provenienti dal controllo, ammesso dal legislatore a tutti i fini contrattuali in sede di procedimento disciplinare e di processo giudiziale, è subordinato al rispetto di alcuni principi, presenti nei provvedimenti dell'Autorità Garante della privacy. Si tratta in primis dei principi di trasparenza e informazione, che implicano consapevolezza del controllato, ma anche di prevenzione, che comporta l'obbligo di adottare misure preventive volte a reprimere comportamenti illeciti e abusivi dei dipendenti, e infine di proporzionalità, che

---

<sup>216</sup> Trib. Napoli, 29 settembre 2010, in Riv. it. dir. lav., 2011, II, 31, con nota di Fusco F., *Il pomo della discordia: il badge come strumento di controllo a distanza?*, in cui si legge che costituiscono strumenti di controllo preterintenzionale a distanza dell'attività dei lavoratori, soggetto alla disciplina dell'art. 4, comma 2, l. 300/1970, un'apparecchiatura di rilevamento delle presenze attivata mediante tessera magnetica, sicché in caso di mancato esperimento della procedura di cui all'art. 4, comma 2, st. lav., non sono utilizzabili in sede disciplinare i dati acquisiti tramite la medesima.

<sup>217</sup> LEVI A. (a cura di), op. cit., il quale si interroga anche sulla natura dell'informativa, o meglio se debba essere concepita come un vero e proprio codice disciplinare, nel quale a ogni singola condotta non ammessa corrisponde una relativa sanzione, oppure debba essere redatta come una policy aziendale. La disposizione non permette di chiarire in modo definitivo tale dubbio interpretativo, in quanto il termine "adeguata" è estremamente generico e l'unica certezza riguarda il carattere necessariamente preventivo dell'informativa

attiene alla modalità di controllo, da non svolgersi mai in modo indiscriminato e senza soluzione di continuità<sup>218</sup>.

La linea direttrice del concetto di trasparenza è meritevole di un approfondimento.

### **3.2 La trasparenza del trattamento delle informazioni registrate**

Dalla ricostruzione del dato normativo emerge come la parola d'ordine adottata dal Legislatore sia “*trasparenza*”: ciò nella convinzione che l'obbligo di rendere edotto il lavoratore in ordine ai controlli a cui è sottoposto costituisca la modalità più efficace per tutelarlo non tanto dal controllo, già avvenuto nel rispetto dei limiti di cui all'art. 4, commi 1 o 2, St. lav., ma dall'impiego delle informazioni per le potenziali ripercussioni sulla figura del lavoratore come parte del rapporto di lavoro.

L'adeguata informazione imposta dall'art. 4, comma 3, St. lav., quale espressione del generale principio di trasparenza del trattamento, dovrà valutarsi caso per caso considerando l'idoneità della stessa di portare a conoscenza del lavoratore, in maniera dettagliata, almeno: a) quali sono gli strumenti, presenti in azienda o utilizzati direttamente o indirettamente dal lavoratore, dai quali può derivare una possibilità di controllo a distanza dell'attività lavorativa; b) quali sono le modalità con le quali è possibile utilizzare gli strumenti forniti dal datore di lavoro, soprattutto con riferimento alla eventuale possibilità di utilizzare quegli stessi strumenti per finalità personali; c) quali sono le modalità con cui potranno essere eseguiti dei controlli sui dati registrati dallo strumento installato in azienda e/o messo a disposizione del lavoratore (quando, come e perché)<sup>219</sup>.

In aggiunta l'obbligo datoriale d'informazione trasparente dovrebbe consentire al lavoratore di riscontrare con maggior facilità eventuali errori o manipolazioni delle informazioni che il datore di lavoro intende utilizzare, acquisendo elementi utili per una sua difesa.

È pur vero che lo strumento attuativo di tale trasparenza, ossia l'informazione al lavoratore, può determinare effetti di altra natura: la preventiva conoscenza della possibilità di essere soggetti a un controllo può svolgere una funzione dissuasiva dal tenere comportamenti illeciti e al tempo stesso può accentuare la condizione di soggezione del lavoratore, anche se in presenza di un controllo legittimo. Tuttavia è proprio l'esigenza di trasparenza di cui si fa portavoce il comma 3 che nell'alternativa tra consapevolezza e non consapevolezza induce a optare per la prima.

La parola-chiave “trasparenza” si trae anche dal quadro europeo.

In un primo momento, infatti, già il principio 3.1 della Raccomandazione del Consiglio d'Europa del 1989, rubricato “*informazione e consultazione dei lavoratori*”, aveva stabilito che,

---

<sup>218</sup> INGRAO A., *Il controllo a distanza effettuato mediante Social network*, in *Labour & Law Issues*, vol. 2, no. 1, 2016.

<sup>219</sup> ALVINO I., op. cit.,

conformemente alla legislazione nazionale e alle disposizioni dei contratti collettivi, i datori di lavoro dovessero informare, preventivamente, i loro lavoratori o i relativi rappresentanti, circa l'introduzione o la modifica di un sistema automatizzato per la raccolta e l'utilizzazione dei dati a carattere personale riguardanti i lavoratori<sup>220</sup>.

Più recentemente, la tematica è stata oggetto di un nuovo intervento a livello comunitario, con la Raccomandazione del Consiglio d'Europa sul trattamento dei dati personali sul posto di lavoro n. 5 del 1° aprile 2015<sup>221</sup>, sostitutiva della raccomandazione del 1989, sostituzione resa necessaria dalla maturata consapevolezza delle intervenute innovazioni tecnologiche.

La Raccomandazione CM/Rec (2015)5 nella sua prima parte (artt. 1 – 13) ribadisce alcuni principi generali in materia di protezione dei dati personali dei lavoratori, con l'obiettivo di ridurre al minimo la circolazione e garantire la maggior trasparenza possibile nel loro utilizzo<sup>222</sup>; la seconda parte (artt. 14 – 21) introduce invece novità di rilievo per quanto riguarda le possibili forme di controllo derivanti dall'utilizzo delle nuove tecnologie, ponendo diverse garanzie a favore dei lavoratori, soprattutto in materia di trasparenza e giustificazione del trattamento dei dati personali connessi all'uso di Internet e posta elettronica.

In particolare la raccomandazione prevede da un lato, al principio n. 5, l'inserimento, all'interno delle policy aziendali, di apposite descrizioni circa le modalità di acquisizione e di conservazione delle informazioni professionali dei lavoratori; dall'altro, al principio n. 21, l'obbligo di informazione preventiva dei lavoratori e di consultazione delle rappresentanze collettive, prima di introdurre qualsiasi tipologia di monitoraggio<sup>223</sup>. E questa proceduralizzazione assume una certa importanza nell'ottica fatta propria dal Consiglio d'Europa, anche alla luce del fatto che essa viene richiamata dal divieto, espresso dal principio n. 15<sup>224</sup>, di introdurre e di utilizzare sistemi

---

<sup>220</sup> Tale norma ha dunque introdotto un principio generale di informazione e consultazione dei lavoratori anticipando di molto la Direttiva 2002/14/CE che individua il quadro generale in materia di diritto all'informazione e alla consultazione dei lavoratori nelle imprese o nelle unità produttive situate in ciascun Paese membro dell'UE.

<sup>221</sup> In quanto raccomandazione è uno strumento la cui attuazione rimane affidata alla volontaria e sovrana scelta degli Stati destinatari, tuttavia occorre tenere conto del fatto che si tratta pur sempre di un atto giuridico formale che, in forma certamente attenuata rispetto alla immediata precettività delle Convenzioni internazionali, obbliga comunque "programmaticamente" gli Stati.

<sup>222</sup> I principi ai quali deve attenersi il datore di lavoro nel trattamento dei dati personali sono quelli del trattamento minimo, ovvero limitato ai dati necessari all'obiettivo da conseguire nel caso specifico, e dello sviluppo di misure idonee ad assicurare l'applicazione dei principi e delle obbligazioni posti dalla raccomandazione; il trattamento dei dati personali inizia al momento della loro raccolta, che l'art. 5 prevede sia fatta al solo diretto interessato; l'uso dei dati personali così raccolti deve essere circoscritto alla finalità specifica che ne ha giustificato la richiesta; per garantire la trasparenza è previsto il diritto di conoscere, direttamente o tramite le rappresentanze sindacali, quali informazioni possiede l'azienda e chi può accedervi, essendo altresì previsto il diritto alla loro rettifica e cancellazione.

<sup>223</sup> Cfr. il testo originale della Raccomandazione del Consiglio d'Europa su <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4224268>.

<sup>224</sup> Nel testo si legge: "Where their introduction and use for other legitimate purpose, such as to protect production, health and safety or to ensure the efficient running of an organisation has for indirect consequence the possibility of monitoring employees' activity, it should be subjected to the additional safeguards set out in principle 21, in particular

informativi e tecnologie con lo specifico e diretto scopo di monitorare l'attività dei lavoratori, presentando una forte assonanza con l'attuale art. 4 St. lav.

In Italia, invece, a sostegno della tesi della preventiva informazione del lavoratore, prima che fosse esplicitamente accolta dall'art. 4 St. lav., giocavano sia alcuni riferimenti normativi, nonché specifiche prassi operative.

Sul piano normativo si segnalano due disposizioni principali: da un lato, l'art. 10, comma 1, della l. 675/1996 che imponeva la preventiva informazione del lavoratore sulle finalità e le modalità del trattamento cui sono destinati i dati; dall'altro, il paragrafo n. 5 dell'allegato XXXIV del d.lgs. 81/2008 che, sulla scia dell'allegato VII par. 3 del d.lgs. n. 626/1994, riguardo all'utilizzo dei videotermini, stabilisce come *“all'atto dell'elaborazione, della scelta, dell'acquisto del software, o allorché questo viene modificato (...) il datore terrà conto che nessun dispositivo o controllo quantitativo o qualitativo può essere utilizzato all'insaputa dei lavoratori”*<sup>225</sup>.

Si tratta di norme fissanti una serie di regole tese a marcare il divieto per il datore di lavoro di compiere controlli occulti, che si rintraccia anche nei provvedimenti emanati dall'Autorità Garante della privacy nel corso del tempo, su tutti le linee guida emanate con deliberazione n. 13 del 1 marzo 2007, al fine di declinare in termini operativi l'utilizzo delle informazioni raccolte per il tramite dell'utilizzo della posta elettronica e di internet, di sistemi di videosorveglianza, dei sistemi di localizzazione dei veicoli e in tema di biometria<sup>226</sup>.

Sul piano delle prassi applicative, invece, bisogna far riferimento alle c.d. policy aziendali e ai codici disciplinari, sedi ideali per stabilire le regole inerenti alle modalità di utilizzo delle strumentazioni dalle quali può scaturire la raccolta di informazioni, in quanto espressione di un giusto bilanciamento tra le diverse esigenze coinvolte. Si tratta di documenti a efficacia interna, vicini al concetto di *soft law* in quanto privi di vincolatività giuridica, con cui il datore di lavoro fissa unilateralmente gli orientamenti di fondo per lo svolgimento dell'attività di impresa e le modalità di utilizzo delle strumentazioni da parte dei dipendenti, con finalità dichiarativa e informativa nei confronti della collettività<sup>227</sup>.

---

*the consultation of the employees' representatives*”. Emerge dunque che la differenza tra la procedura consultiva prevista dal principio n. 15 della Raccomandazione e l'art. 4 St. lav. risiede nell'attribuzione alla contrattazione collettiva gestionale di un ruolo di chiusura non imposto *a priori*, ma solamente qualora se ne ravvisi l'opportunità nel corso della procedura di consultazione. Sul punto, SITZIA A., *I controlli a distanza dopo il “Jobs Act” e la Raccomandazione R(2015)5 del Consiglio d'Europa*, in LG, 2015, pp. 671 ss.

<sup>225</sup> CHIECO P., *Telelavoro e statuto dei lavoratori*, in Lav. inf., 1999, n. 12.

<sup>226</sup> Cfr. GRAGNOLI E., *L'uso della posta elettronica sui luoghi di lavoro e la strategia di protezione elaborata dall'autorità garante*, Padova, 2010; TULLINI P., *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. Uso di mezzi elettronici, potere di controllo e trattamento dei dati personali in Trattato di diritto commerciale e di diritto pubblico dell'economia*, Padova, 2010; PAISSAN M., *Email e navigazione in internet: le linee guida del Garante* in TULLINI P., *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, Padova, 2010.

<sup>227</sup> MONTEMANARO A., *Il codice di comportamento dei dipendenti pubblici*, in Guida lav., 2013, n. 27.

Le policy devono essere portate a conoscenza del lavoratore attraverso un'informazione preventiva e, in tal modo, il dipendente viene coinvolto direttamente e personalmente negli obiettivi dell'azienda, al fine di svolgere un'attività lavorativa più efficiente ed efficace, orientando la propria condotta alle linee guida di fondo fissate dall'impresa.

### **3.3 La tutela della privacy: la seconda condizione dell'utilizzabilità dei dati raccolti**

La raccolta delle informazioni tramite controlli a distanza si caratterizza per un altro limite di utilizzabilità, oggi sancito direttamente e sempre dall'art. 4, comma 3, St. lav. e si tratta del rinvio al *“rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196”*.

Tale disposizione sancisce espressamente il doppio binario di tutela in materia; doppio binario che, da sempre, o quantomeno dalla prima normativa in materia di privacy, ha caratterizzato la disciplina dell'utilizzo dei dati raccolti tramite strumenti di controllo del datore di lavoro.

Il rinvio a quanto disposto dal d.lgs. 196/2003 testimonia definitivamente l'intersecazione dei due diversi piani regolativi dei controlli a distanza: da un lato, quello statutario, tipicamente lavoristico, dall'altro, quello della tutela della riservatezza, tipicamente civilistico<sup>228</sup>.

La norma pone un interrogativo fondamentale legato al ruolo proprio di tale rinvio formale e al suo *“essere sufficiente”* per l'integrazione dei due sistemi regolativi.

La risposta fornita è stata diversa a seconda del momento storico in cui ci si è interrogati sulla questione.

I primi commentatori, infatti, essendosi concentrati sul significato politico della riforma e sull'enfatizzare l'obiettivo legislativo primario di rinnovamento di un testo obsoleto, rimasto inalterato dal 1970, avevano ritenuto la prospettiva generale del raccordo con le regole di tutela della privacy secondaria, se non meramente eventuale. In un secondo momento, invece, la dottrina ha definito il nuovo art. 4 St. lav. come un *“puzzle di disposizioni diverse”*<sup>229</sup>, dal diverso valore cogente, destinato a comporsi nel corso del tempo grazie all'intervento direttivo dell'Autorità garante per la privacy e dell'interpretazione giurisprudenziale.

La riforma dell'art. 4 St. lav. ha in parte confuso il sistema di rinvio tra i due apparati normativi in quanto oggi la norma precisa, come già ricordato, che le informazioni raccolte ai sensi dei commi 1 e 2 dell'art. 4 St. lav. sono utilizzabili, previa adeguata informativa, solo ai fini connessi al rapporto di lavoro, a condizione che sia rispettato quanto disposto dal Codice della privacy. Questa modifica normativa crea un circuito di rimandi legislativi che rende arduo capire con certezza quali siano i

---

<sup>228</sup> ICHINO P., *Il contratto di lavoro*, in CICU A. – MESSINEO F., *Trattato di diritto civile e commerciale*, III, Milano, 2003.

<sup>229</sup> LEVI A. (a cura di), *op. cit.*

rapporti tra regola generale e speciale, cosicché, come ritenuto in dottrina, il compito di coordinare l'art. 4 con la disciplina in materia di dati personali è lasciato all'interprete<sup>230</sup>.

Non si può però parlare del d.lgs. n. 196/2003, senza tenere in considerazione la recente modifica da cui è stato investito, modifica apportata dal d.lgs. n. 101/2018, volto ad adeguare il Codice della privacy al regolamento europeo n. 679/2016.

L'attuale quadro normativo in materia di protezione dei dati personali in Italia si articola dunque su due livelli formati e, dal regolamento europeo sulla privacy e, dal Codice privacy novellato dal d.lgs. 101/2018.

È opportuno segnalare che la normativa italiana va interpretata e applicata conformemente a quella europea, in quanto integra ma non sostituisce il Regolamento n. 679/2016. L'art. 288 TFUE statuisce che ciascun regolamento europeo, e pertanto anche il Regolamento 679/2016, ha portata generale, è obbligatorio in tutti i suoi elementi ed è direttamente applicabile in ciascuno degli stati membri.

### **3.3.1 Il Regolamento (UE) n. 679/2016 e il d.lgs. n. 101/2018: i due poli della tutela della riservatezza in materia di controllo a distanza**

La legge delega 183/2014, base dell'intera riforma del Jobs Act, non faceva alcun cenno all'integrazione della specifica materia in commento tra livello regolativo nazionale e livello sovranazionale e, difatti, i decreti legislativi del 2015 non sono maturati in un contesto di stretta armonizzazione.

Nonostante ciò, l'interpretazione del doppio binario normativo che si desume dall'art. 4, comma 3, St. lav., ad oggi, rappresenta un settore foriero di questioni interpretative, anche sul piano della c.d. privacy multilivello.

Non si può prescindere, difatti, dall'analisi dell'evoluzione europea del quadro normativo in materia di tutela della riservatezza e, in particolare, dal nuovo Regolamento europeo generale sulla protezione dei dati (GDPR) n. 679 del 2016<sup>231</sup>, regolamento in materia di trattamento dei dati personali e di privacy, che ha sostituito i contenuti della direttiva 95/46/CE, esaminata nel precedente capitolo e, in Italia, ha abrogato gli articoli del Codice privacy con esso incompatibili.

Pur ponendosi in un certo senso in un'ottica di formale continuità con la previgente disciplina in materia, tanto che *“il Regolamento, così come la precedente Direttiva 95/46/CE, costituisce un vero*

---

<sup>230</sup> ALVINO I., op.cit.

<sup>231</sup> Il regolamento è stato adottato il 27 aprile 2016, pubblicato sulla Gazzetta ufficiale dell'Unione europea il 4 maggio 2016, entrato in vigore il 24 maggio dello stesso anno ed è divenuto operativo a partire dal 25 maggio 2018.

*e proprio statuto dell'informazione che trae la sua ratio dal fatto che il dato personale è un frammento dell'individuo che a esso appartiene in virtù di una relazione quasi dominicale e, come tale, richiede protezione quando coinvolto in processi circolatori vorticosi*<sup>232</sup>, al tempo stesso esso introduce rilevanti novità, rappresentando un punto di svolta nel panorama normativo. È innegabile come il Regolamento infatti si proponga anche e soprattutto quale elemento di superamento di una precedente frammentazione giuridica delle norme e della prassi applicativa in tema di protezione di dati personali.

Ai fini dell'analisi condotta nel presente elaborato, è opportuno porre particolare attenzione sull'art. 88 del regolamento, rubricato *“trattamento dei dati nell'ambito dei rapporti di lavoro”*.

Il GDPR non detta norme specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, rinviando agli Stati membri o alla contrattazione collettiva la possibilità di una loro introduzione<sup>233</sup>. L'art. 88 prevede puntualmente che: *“Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro 25 maggio 2018 e comunica senza ritardo ogni successiva modifica”*.

---

<sup>232</sup> INGRAO A., *Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy*, in *Labour & Law Issues*, vol. 5, n. 2, 2019, p. 138.

<sup>233</sup> Nel Considerando n. 155 si legge: *“Il diritto degli Stati membri o i contratti collettivi, ivi compresi gli accordi aziendali, possono prevedere norme specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per quanto riguarda le condizioni alle quali i dati personali nei rapporti di lavoro possono essere trattati sulla base del consenso del dipendente, per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro”*.

In particolare, dunque, ai sensi dell'art. 88 GDPR, possono essere adottate norme di diritto interno al fine di assicurare una maggiore protezione al lavoratore sia in relazione al trattamento finalizzato all'instaurazione e cessazione del rapporto di lavoro, sia per quello relativo alla esecuzione del contratto di lavoro e all'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi<sup>234</sup>. Norme specifiche possono anche essere previste per finalità di pianificazione e organizzazione del lavoro, nonché per quelle relative alla parità sul posto di lavoro ed alla prevenzione dei rischi in materia di salute o alla protezione della proprietà del datore di lavoro o del cliente.

In ciascuno dei casi previsti dall'art. 88 GDPR, le discipline legali interne dovranno includere misure a tutela della privacy, con riferimento alla trasparenza del trattamento, nonché al trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune. Infine, particolare attenzione è data dal Legislatore europeo alle modalità di utilizzo dei dispositivi, hardware e software, attraverso i quali sia possibile il monitoraggio del personale dipendente.

Si tratta di una disposizione dotata di una grande chiarezza espositiva, che induce immediatamente a riflettere sui futuri rapporti tra tali punti di diritto e la disciplina interna, identificabile con il Codice privacy del 2003.

In materia di trattamento nell'ambito dei rapporti di lavoro, il Codice privacy si mostra molto specifico nel delineare obblighi e adempimenti a carico del datore di lavoro, affinché il trattamento dei dati dei dipendenti possa effettuarsi nella completa liceità e correttezza.

Gli interpreti<sup>235</sup>, pertanto, ritengono che il Codice privacy possa continuare, in futuro, a sortire i propri effetti, anche a seguito dell'applicazione diretta da parte dell'Italia del Regolamento n. 679/2016, pur considerando la possibilità, a discrezione degli Stati membri, di maggiori specificazioni tese ad assicurare completamente e meglio i principi europei. Una lettura ormai confermata dalle scelte operate nell'aggiornamento del testo del d.lgs. 196/2003.

Nel Codice privacy, oggi, per la tutela della riservatezza nell'alveo dei controlli a distanza del datore di lavoro, si rinvia esplicitamente alle garanzie dell'art. 4 St. lav. tramite l'art. 114 del Codice, che trova il suo fondamento nei principi espressi nell'art. 2-sexies, rubricato "*trattamento di*

---

<sup>234</sup> Il trattamento dei dati dei lavoratori con la finalità di assunzione esula dall'oggetto del presente lavoro. Tuttavia, tale genere di operazioni di trattamento dei dati da parte dei datori di lavoro è molto frequente, in particolare grazie all'utilizzo di social network, professionali (come LinkedIn) o generici (come Facebook, Instagram, Twitter). Per un'analisi di tipo statistico sull'utilizzo del social recruiting da parte delle imprese italiane, dettagliata e divisa per settore merceologico, cfr. il Report dell'Osservatorio sulle competenze digitali 2018, realizzato da Aica, Anitec-Assinform, Assintel, Assinter, con il supporto di CFMT, Confcommercio, Confindustria e in collaborazione con AgID - Agenzia per l'Italia Digitale e Ministero dell'Istruzione dell'Università e della Ricerca, su <https://www.lispa.it>.

<sup>235</sup> Cfr. GAMBA C., *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove*, in Labour&Law Issues, Vol. 2, n. 1, 2016; LONGO A., *GDPR – Tutto ciò che c'è da sapere per essere in regola*, su <https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-dasapere-per-essere-preparati/>.

*categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante”* che, alla lettera dd), fa riferimento a *“instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili (...)”*.

La disciplina in materia di protezione di dati personali svolge, senz'altro, una funzione contenitiva degli abusi datoriali e delle potenzialità di invasione/lesione dei “beni personali” (dignità, riservatezza, ecc.) dei lavoratori, nel controllo sugli strumenti di lavoro.

Il datore di lavoro, ai fini della legittimità della raccolta e del trattamento delle informazioni sui lavoratori, è obbligato a osservare l'articolato apparato di regole, sostanziali e procedurali, in materia di protezione dei dati personali, dettate dal d.lgs. n. 196/2003: in parte generali, ossia applicabili a tutti i tipi di trattamenti di dati; in parte differenziate per i dati comuni, sensibili e giudiziari, e a seconda che il titolare del trattamento sia un soggetto (datore di lavoro) privato o pubblico (con un diverso regime di tutela per i lavoratori privati e per i pubblici dipendenti); infine, speciali per peculiari tipi di trattamenti dei dati (come, ad esempio, quelle riguardanti la fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni: artt. 121 ss.)<sup>236</sup>. Tale regolamentazione è corredata da sanzioni civili, da sanzioni penali e amministrative<sup>237</sup>.

Accanto alle regole di fonte legislativa, il datore di lavoro è obbligato a osservare quelle dettate dalla normativa sia regolamentare, sia emanata dall'Autorità Garante della privacy, nell'esercizio del suo potere “normativo”, in particolare sotto forma di autorizzazioni generali, linee guida (tra cui, sulle nuove tecnologie nel lavoro: linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati, del 23 novembre 2006; linee guida per posta elettronica e internet, del 1° marzo 2007), e provvedimenti generali (specialmente il provvedimento generale dell'8 aprile 2010, in materia di videosorveglianza; e il provvedimento generale 4 ottobre 2011, n. 370, concernente i sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro).

L'applicazione della normativa sulla protezione dei dati personali produce, in particolare, l'effetto di circoscrivere il potere del datore di lavoro di compiere qualunque operazione di elaborazione elettronica dei dati (anche dei lavoratori), immagazzinati o meno in banche di dati aziendali e in

---

<sup>236</sup> TROJSI A., *Il diritto del lavoratore alla protezione dei dati personali*, Torino, 2013.

<sup>237</sup> Sul punto cfr. FLOR R., *Diritto penale e controlli a distanza dei lavoratori dopo il Jobs Act*, in LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza*, Milano, 2016; GROTTO M., *La rilevanza penale del controllo datoriale attraverso gli strumenti informatici*, in *Dir. inf.*, 2014, p. 57.

archivi informatici. Del resto, la *ratio* originaria dell'introduzione, a livello europeo, nonché nazionale, di regole sulla circolazione dei dati personali è stata proprio quella di disciplinare il trattamento dei dati automatizzato, ossia effettuato mediante strumenti elettronici.

L'esercizio del potere di controllo del datore di lavoro deve, inoltre, avvenire in ossequio ai principi di cui all'art. 5 GDPR rubricato "*principi applicabili al trattamento di dati personali*".

Tale disposizione impone il rispetto dei principi di liceità, correttezza, trasparenza ed esattezza, richiedendo che i dati personali siano trattati in modo lecito, corretto, trasparente ed esatto nei confronti dell'interessato; che siano raccolti per finalità determinate esplicite e legittime, e coerenti con tali scopi, nel rispetto del principio di limitazione della finalità; che siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, nel rispetto del principio di minimizzazione dei dati.

Prima dell'ingresso del regolamento europeo in questione, analoghi principi erano già espressi dal Codice privacy.

L'art. 3 era rubricato "*principio di necessità nel trattamento dei dati*" e sanciva che "*i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*".

L'art. 11 era rubricato "*modalità del trattamento e requisiti dei dati*" e, se nel comma 1 esplicava i vari dati oggetto del trattamento, al comma 2 prescriveva che "*i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*".

Le due disposizioni sono state abrogate per effetto del d.lgs. 101/2018 e ricomprese nel menzionato art. 5 GDPR.

Quanto detto evidenzia come il Legislatore italiano abbia proceduto all'armonizzazione del Codice privacy con il regolamento europeo: attraverso l'emanazione del d.lgs. n. 101/2018 ha provveduto a modificare, e in gran parte abrogare, le disposizioni del d.lgs. n. 196/2003<sup>238</sup>.

Nel nuovo testo del Codice privacy non si rinvencono disposizioni di particolare rilievo in materia di controllo a distanza, bensì un laconico rinvio all'art. 4 St. lav.<sup>239</sup>.

In particolare, tra le maggiori novità in materia apportate dal d.lgs. poc'anzi menzionato, autore dell'emendamento, vi sono gli artt. 113 e 114 del Codice privacy, a mente dei quali rispettivamente

---

<sup>238</sup> L'attuale art. 1 d.lgs. n. 196/2003 prescrive che il trattamento dei dati personali deve avvenire secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.

<sup>239</sup> Ex art. 114 Codice privacy, "*resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300*"

rimane fermo quanto disposto dagli artt. 8, a cui viene aggiunto *ex novo* l'art. 10 d.lgs. n. 276/2003<sup>240</sup>, e art. 4 St. lav.

L'art. 113, che conferma il principio in base al quale il datore di lavoro non può tenere conto di informazioni personali del lavoratore prive di uno stretto collegamento con il rapporto di lavoro e con l'esecuzione del contratto, è contenuto nel capo II, modificato da “*annunci di lavoro e dati riguardanti prestatori di lavoro*” a “*trattamento di dati riguardanti i prestatori di lavoro*”.

La modifica a cui è poi sottoposto l'art. 114 investe sia la sua stessa rubrica, che il capo in cui è contenuta la norma: la disposizione passa da essere rubricata “*controllo a distanza*” a “*garanzie in materia di controllo a distanza*” e il capo III, in cui è inserita, muta da “*divieto di controllo a distanza e lavoro agile*” a “*controllo a distanza, lavoro agile, e telelavoro*”.

Per il resto, il titolo VIII del d.lgs. n. 196/2003, dedicato ai “*trattamenti nell'ambito del rapporto di lavoro*”, contiene una scarsa disciplina, essenzialmente di rinvio ad altre disposizioni. Rispetto alla tematica trattata, alcuni ulteriori profili di interesse possono rinvenirsi soltanto nell'art. 111 d.lgs. n. 196/2003, che oggi attribuisce al Garante il compito di promuovere l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.

La nuova formulazione abbandona l'idea del “*codice di deontologia e buona condotta*”<sup>241</sup>, individuando una libertà delle forme per la raccolta e la formulazione delle stesse, e ribadisce la

---

<sup>240</sup> La disposizione recita così: “*E' fatto divieto alle agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonché ad eventuali controversie con i precedenti datori di lavoro, a meno che non si tratti di caratteristiche che incidono sulle modalità di svolgimento dell'attività lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa. È altresì fatto divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo. Le disposizioni di cui al comma 1 non possono in ogni caso impedire ai soggetti di cui al medesimo comma 1 di fornire specifici servizi o azioni mirate per assistere le categorie di lavoratori svantaggiati nella ricerca di una occupazione*”.

<sup>241</sup> Cfr. BUSIA G., *Codici di deontologia e buona condotta, Commento all'art.12*, in *Codice della privacy*, Commentario coordinato da ITALIA V., *Le nuove leggi amministrative*, 2004, 166; DE MINICO G., *Codici di deontologia e buona condotta, Commento all'art. 12*, in *La protezione dei dati personali, Commentario al d.lgs. 30 giugno 2003, n. 196 (“Codice della privacy”)* BAINCA M. – BUSNELLI F.D. (a cura di), *Le nuove Leggi Civili Commentate*, tomo I, Padova, 2007, pp. 271 ss. I codici di buona condotta nascono dall'art. 27 della direttiva n. 95/46/CE, che promuove l'adozione di codici di condotta per “*contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione*” della Direttiva stessa.

L'art. 12 del Codice privacy (sostitutivo dell'art. 31 L. n. 675/1996) attribuiva, prima di essere abrogato dal d.lgs. n. 101/2018, al Garante il potere di incentivare la sottoscrizione di codici di deontologia e buona condotta, nell'ambito delle categorie interessate, di verificarne la conformità alle leggi e ai regolamenti.

Dal raffronto dalle due normative emerge come a livello comunitario ai codici fosse attribuito un ruolo più ridotto rispetto a quello da loro svolto nel nostro ordinamento.

necessità di un'informazione adeguata al lavoratore<sup>242</sup>. Nelle more di una specifica disciplina di diritto interno, dunque, la liceità del trattamento dei dati dei lavoratori andrà verificata alla luce delle regole generali e delle condizioni dettate dalla norma regolamentare.

Secondo l'art. 6 GDPR, inoltre, ogni titolare del trattamento dovrà in primis accertarsi che le relative operazioni abbiano base giuridica in una delle seguenti ipotesi: a) il consenso del lavoratore; b) la necessità del trattamento ai fini dell'esecuzione del rapporto contrattuale di cui l'interessato è parte; c) l'adempimento di un obbligo legale al quale è soggetto il datore di lavoro; d) la necessità del trattamento ai fini della salvaguardia di un interesse vitale del lavoratore; e) l'esecuzione di un compito di interesse pubblico; f) il perseguimento del proprio legittimo interesse, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali del lavoratore.

Il rispetto degli adempimenti e delle prescrizioni privacy quale condizione imprescindibile per l'utilizzabilità delle informazioni raccolte nei luoghi di lavoro tramite strumenti tecnologici, previsto dall'art. 4, comma 3, St. Lav., impone innanzitutto l'individuazione delle condizioni di liceità del trattamento dati implicato nell'esercizio del potere di controllo.

Tale attività interpretativa, però, presenta profili problematici di non poco conto.

In primo luogo, la circostanza per la quale il rapporto di lavoro abbia fonte negoziale non pare sufficiente a legittimare il trattamento occasionato dall'attività di controllo a distanza, in quanto tra le esigenze che a questo sottendono e l'esecuzione del rapporto contrattuale di lavoro non è sempre rinvenibile l'esistenza di un nesso di causalità, tale per cui la mancanza del trattamento dati comporterebbe l'impossibilità di esecuzione del contratto. Confortano l'assunto, peraltro, le indicazioni già fornite dal Gruppo di lavoro *ex art. 29* (detto anche Working Party art. 29, WP29)<sup>243</sup>,

---

Nel sistema della Direttiva Comunitaria, i codici si limitavano a contribuire alla corretta applicazione delle disposizioni in materia di tutela dei dati attraverso la specificazione della normativa all'interno dei vari settori, con lo scopo di facilitazione e non di integrazione o sostituzione della normativa; nel nostro ordinamento ai codici di deontologia e buona condotta, al contrario, è stato affidato una funzione sostitutiva dei decreti legislativi che il Governo avrebbe dovuto emanare prima dell'emanazione del d.lgs. n. 196/2003.

<sup>242</sup> Cfr. RICCIO G.M. - SCORZA G. - BELISARIO E. (a cura di), *GDPR e normativa privacy. Commentario*, Milanofiori Assago (MI), 2018.

<sup>243</sup> Le funzioni consultive e di indirizzo in materia di protezione dei dati personali venivano svolte, in vigenza della direttiva 95/46/CE, dal Gruppo di lavoro *ex art. 29*, detto anche Working Party art. 29 (noto con l'acronimo WP29), ovvero un organismo indipendente, composto da un rappresentante delle varie autorità nazionali in materia, in ambito europeo. A seguito dell'entrata in vigore del Regolamento europeo n. 679/2016, il WP29 è stato sostituito dal Comitato europeo per la protezione dei dati (Edbp), che è un organo europeo indipendente avente oltre alle medesime funzioni consultive e di indirizzo ulteriori compiti di garanzia della uniforme applicazione del regolamento in ambito europeo anche attraverso la promozione della cooperazione tra le autorità competenti per la protezione dei dati dell'UE. Il Comitato europeo si è riunito per la prima volta il 25 maggio 2018 approvando gli orientamenti relativi al regolamento generale sulla protezione dei dati (GDPR) forniti dal WP29, al contempo cessandone di fatto le attività.

per il quale la base giuridica “*non si applica a tutte le ulteriori azioni avviate a seguito di inosservanza o a tutti gli altri incidenti intervenuti nell’esecuzione di un contratto*”<sup>244</sup>.

Anche l’ulteriore fondamento giuridico rinvenibile nell’adempimento di obblighi legali si adatta difficilmente alla fattispecie che qui si analizza. Infatti, configurandosi per lo più come esercizio facoltativo di potere, soltanto in ipotesi circoscritte l’attività di controllo trova la propria base giuridica in un obbligo legale al quale è soggetto il titolare del trattamento, come accade, ad esempio, con gli apparecchi di controllo nel settore del trasporto su strada (dispositivi cronotachigrafi), in ossequio al Regolamento 561/2006/CE, come modificato dal Regolamento europeo 165/2014/CE, o come accade con i sistemi di localizzazione GPS dei veicoli portavalori, ai sensi dell’allegato D, art. 257 Testo unico delle leggi di pubblica sicurezza (T.U.L.P.S.)<sup>245</sup>.

In proposito sembra potersi affermare che la comprovata esistenza di esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, ovvero la necessità di adottare strumenti tecnologici per rendere la prestazione lavorativa, secondo quanto previsto proprio dall’art. 4 St. lav., non sia altro che una specificazione legale del legittimo interesse richiamato dal GDPR. Tale approccio interpretativo, peraltro, è avvalorato dal Considerando n. 47 GDPR, secondo il quale i legittimi interessi di un titolare del trattamento “*possono costituire una base giuridica del trattamento*”, sussistendo “*quando esista una relazione pertinente e appropriata tra l’interessato e il titolare del trattamento, ad esempio quando l’interessato è (...) alle dipendenze del titolare del trattamento*” ma “*a condizione che i legittimi interessi del titolare non prevalgano (su) gli interessi o i diritti e le libertà fondamentali dell’interessato, tenuto conto delle ragionevoli aspettative nutrite dall’interessato in base alla sua relazione con il titolare del trattamento*”. La presenza dell’inciso “a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali” dell’interessato impone al datore di lavoro, intenzionato a porre il proprio legittimo interesse a fondamento del trattamento, di valutarne attentamente l’incidenza sulla sfera di riservatezza del lavoratore<sup>246</sup>.

---

<sup>244</sup> Cfr. WP217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, pp. 20, 21. Secondo il gruppo di lavoro “*il monitoraggio elettronico dell’utilizzo di Internet, della posta elettronica o del telefono da parte dei dipendenti o la videosorveglianza dei lavoratori costituiscono più chiaramente trattamenti che con ogni probabilità vanno oltre quanto necessario all’esecuzione di un contratto di lavoro, sebbene anche in questo caso ciò possa dipendere dalla natura dell’attività lavorativa*”.

<sup>245</sup> L’Ispettorato nazionale del lavoro ha fornito chiarimenti in merito all’installazione di apparecchiature di localizzazione satellitare GPS con la circ. 2/2016.

<sup>246</sup> Nel Considerando 47, si legge: “*in ogni caso, l’esistenza di legittimi interessi richiede un’attenta valutazione anche in merito all’eventualità che l’interessato, al momento e nell’ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell’interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali*”. Tale previsione appare espressione del più generale principio di “accountability” o “responsabilizzazione” del titolare del trattamento, esplicitato all’art. 5, par. 2 GDPR, ai sensi del quale gli viene

In particolare, il metodo scelto o la tecnologia specifica con cui verrà effettuato il trattamento deve essere necessario per il perseguimento del legittimo interesse del datore di lavoro e il trattamento deve essere proporzionato alle esigenze aziendali, in ossequio ai principi di minimizzazione e di limitazione della finalità previsti dall'art. 5 GDPR<sup>247</sup>.

### 3.3.2 Privacy by default e privacy by design

Nel nuovo scenario tecnologico, il Regolamento fa un salto rispetto alla previgente direttiva del 1995, appropriandosi di una filosofia regolativa incentrata sul concetto di “rischio”.

Il Regolamento altro non è che una complessa architettura regolativa rivolta a prevenire, e se possibile impedire, le conseguenze negative scaturenti, sulla persona, dall'uso massiccio della tecnologia che consente di raccogliere, immagazzinare, rielaborare e conservare dati eterogenei e di utilizzarli per gli scopi più disparati.

La grande rivoluzione compiuta dal GDPR consiste soprattutto in questo “cambio di prospettiva” sul quale poggia l'intero impianto strutturale del regolamento: a differenza della direttiva 95/46/CE, il cui nucleo principale era rappresentato dai diritti dell'interessato (cd. *data subject*), il Regolamento trova il suo perno nel titolare del trattamento dei dati personali, che risulta destinatario di una serie di doveri e responsabilità. A tal riguardo, uno dei pilastri del Regolamento, che fa da architrave a questa imponente costruzione, è il principio di “*accountability*”<sup>248</sup>, tradotto impropriamente in italiano come “responsabilizzazione”, in virtù del quale il titolare del trattamento, operando in un'ottica proattiva, effettua anticipatamente un'attenta analisi del rischio, volta a prevenire eventuali violazioni di diritti e libertà degli interessati, che possano discendere da un improprio utilizzo dei loro dati personali, con il successivo duplice obbligo e, di dimostrare di avere a tal fine adottato misure tecniche e organizzative adeguate riguardo alle peculiarità e ai

---

demandata la capacità di comprovare il rispetto della normativa. A tal fine si rende necessario, per ogni titolare del trattamento, un'attività di audit di processi interni che, partendo da un'analisi del rischio, metta in atto politiche adeguate di protezione dei dati. Sul tema in CARNABUCI A. - CECCOLI P. - DE ROSA B. - MARIANI I. - MINIERI C. - RADAELLI P. - ZAPPIA A. - ZUCCHETTI A., *Privacy e dati personali: problemi e casi pratici*, Milano, 2018.

<sup>247</sup> Sulle specificità del trattamento basato sul legittimo interesse del datore di lavoro, cfr. Gruppo di lavoro Art. 29, Parere 2/2017 sul trattamento dei dati sul posto di lavoro, 8 giugno 2017 e Gruppo di lavoro Articolo 29, Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'art. 7 della Direttiva 95/46/CE, 9 aprile 2014

<sup>248</sup> Si rimanda all'art. 24 del Regolamento (UE) 2016/679 che così recita: “1. *Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*”. Sul punto anche IBBA F. G., *GDPR, il rapporto tra privacy, trasparenza amministrativa e accountability*, in Agenda Digitale, 2018.

bisogni della singola organizzazione, e, di garantire l'efficace attuazione delle regole poste dal regolamento. L'adeguatezza di tali misure deve essere valutata con riferimento non soltanto alla fase di svolgimento del trattamento, ma anche e soprattutto al momento della progettazione del trattamento medesimo.

L'idea che la tutela dei diritti e delle libertà degli interessati, con riguardo al trattamento dei dati personali, debba comportare l'adozione e l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione, che dell'esecuzione del trattamento stesso trova la propria consacrazione nel principio della cosiddetta "*privacy by design*"<sup>249</sup>.

Tale principio, teorizzato ed elaborato per la prima volta dalla Dott.ssa Ann Cavoukian<sup>250</sup>, benché già in precedenza ufficializzato nella risoluzione del 2010 della trentaduesima Conferenza mondiale dei Garanti, entra nel quadro normativo europeo proprio mediante il regolamento. A esso il GDPR affianca, in un binomio indissolubile, il principio di "*privacy by default*"<sup>251</sup>, il quale prevede che, per impostazione predefinita, sia raccolta e utilizzata la minore quantità possibile di dati personali, limitando il trattamento a quei soli dati che risultino pertinenti e strettamente necessari al raggiungimento delle finalità perseguite.

I principi di *privacy by design* e *privacy by default* assumono, nell'odierna società digitalizzata, una rilevanza sempre crescente.

L'introduzione della tecnologia in azienda deve rispondere ai dettami della *privacy by design* e *by default* che, assunto il carattere conformativo della tecnologia, mai neutra piegandosi al volere di chi ne decide l'impostazione, obbligano a incorporare le regole di protezione dei dati dei lavoratori all'interno della strumentazione aziendale e a mantenerle per tutto il ciclo di vita dei trattamenti.

Con lo sviluppo di strumenti tecnologici sempre più ricercati, capaci di raccogliere ed elaborare, in totale autonomia, prescindendo da ogni intervento umano, ingenti quantità di dati riferiti o riferibili a soggetti individuati, sottoponendo questi ultimi a un controllo capillare e, sempre più spesso, occulto, è emersa l'esigenza di incorporare misure a tutela della *privacy* sin dalla fase di progettazione di tali strumenti, rendendoli idonei a realizzare un trattamento dei dati quanto più rispettoso dei diritti e delle libertà degli individui interessati dal trattamento medesimo.

E guardando al soggetto come lavoratore ciò è tanto più vero: in tale veste, l'individuo condivide una notevole mole di informazioni a lui inerenti. Tali informazioni, in una realtà come quella in cui viviamo oggi, dove il prestatore di lavoro, nell'eseguire le proprie mansioni, si avvale sempre più frequentemente di dispositivi elettronici e sistemi informatici, il più delle volte messi a disposizione

---

<sup>249</sup> Cfr. art. 25, comma 1, del Regolamento (UE) 2016/679.

<sup>250</sup> La Dott.ssa Ann Cavoukian, cui si deve la formulazione del concetto di *privacy by design*, è stata dal 1997 al 2014 Commissario per le Informazioni e la Privacy della provincia canadese dell'Ontario.

<sup>251</sup> Cfr. art. 25, comma 2, del Regolamento (UE) 2016/679.

dall'azienda stessa per la quale lavora, non sono più solo quelle raccolte in occasione dell'assunzione e dell'esecuzione del contratto di lavoro, per l'eventuale adempimento di obblighi previsti dalla legge o da contratti collettivi (come generalità, dati sanitari, dati giudiziari), ma comprendono anche quelle accidentalmente lasciate dal lavoratore durante la navigazione sul web, quelle connesse allo scambio di email o quelle presenti sui social network. Il rischio che siano in tal modo acquisite informazioni personali, non rilevanti ai fini della valutazione della professionalità del prestatore, in potenziale violazione dell'articolo 8 St. lav., è elevato, tanto più nel caso in cui gli strumenti possano essere utilizzati in modo promiscuo dal lavoratore, e quindi anche al di fuori dell'orario di lavoro. Altrettanto elevato è il rischio che dall'impiego di siffatta strumentazione possa derivare un controllo indiscriminato e costante sull'attività dei dipendenti, potenzialmente lesivo della libertà e dignità di questi ultimi, e perciò assoggettabile alla disciplina di cui all'articolo 4 St. lav.

L'invito rivolto ai datori di lavoro, e, in prima battuta, ai fornitori dei servizi e degli strumenti di cui essi si avvalgono nella gestione e nell'organizzazione del rapporto di lavoro è, pertanto, quello di adottare misure e accorgimenti finalizzati a congegnare tali strumenti e servizi in maniera da tale da, se non eliminare, quantomeno ridurre drasticamente i rischi connessi a un utilizzo illecito dei dati personali dei lavoratori, in ossequio al principio della *privacy by design* (e, di riflesso, della *privacy by default*)<sup>252</sup>.

Mettere in pratica le novità introdotte dal Regolamento (UE) 2016/679, specie quelle in tema di *privacy by design* e *privacy by default*, non è sempre facile. L'interrogativo che attanaglia quanti, a seguito dell'entrata in vigore del GDPR, sono tenuti ad adeguarsi alla nuova disciplina normativa, è, non a caso, legato al come applicare e integrare i principi suddetti. A tal riguardo potrebbe rivelarsi utile tracciare delle linee guida, rendendo più agevole l'adozione di adeguate misure tecniche e organizzative, per dotare il sistema di meccanismi in grado di condurre a buon fine il trattamento dei dati.

In particolare, il principio di *privacy by design*, come detto, si traduce nell'obbligo di incorporare le misure di sicurezza direttamente in applicazioni, servizi e prodotti destinati a essere utilizzati per fini di trattamento di dati personali, sin dalla fase della loro progettazione.

Nell'ottica del rapporto tra datore di lavoro e lavoratore, che in questa sede interessa, i sistemi dovrebbero essere progettati in maniera tale da operare, anche in via automatica, una selezione delle

---

<sup>252</sup> Cfr. CAVOUKIAN A., *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D*, in *Identity in the Information Society*, vol. 3, 2010, pp. 247-251; CALZOLAIO S., *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, su <http://www.federalismi.it/>, 2017; PAGALLO U., *Privacy e design*, in *Informatica e diritto*, vol. XVIII, no. 1, 2009.

informazioni raccolte, evitando l'utilizzo e la diffusione di dati non rilevanti ai fini della gestione e organizzazione del rapporto di lavoro. Ove possibile, sarebbe preferibile ricorrere a tecniche di pseudonimizzazione e cifratura (o crittografia) dei dati. Tali tecniche si pongono tra loro in un rapporto di "mezzo a fine": con l'ausilio di tecniche di cifratura è possibile, infatti, ottenere dati "pseudonimi", per tali intendendosi dati non direttamente riferibili a un interessato specifico senza l'utilizzo di informazioni aggiuntive, le quali, a loro volta, devono essere conservate separatamente. È altresì buona prassi evitare che i dati personali siano conservati per un lasso temporale troppo ampio, configurando, ad esempio, il sistema in modo tale da disporre la cancellazione automatica dei dati, decorso un certo periodo<sup>253</sup>.

La predisposizione di misure di tutela della privacy sin dalla fase di progettazione non dispensa tuttavia il datore di lavoro titolare del trattamento dal predisporre test, verifiche e valutazioni periodiche volte ad accertare l'efficacia delle misure tecniche e organizzative allo scopo di garantire la sicurezza del trattamento<sup>254</sup>.

Un settore problematico per il trattamento di dati personali dei dipendenti è quello del monitoraggio del traffico internet. Già prima dell'entrata in vigore del regolamento europeo, il Garante era intervenuto sulla questione con provvedimento n. 65 del 5 febbraio 2015,<sup>255</sup> reso a seguito di un reclamo promosso da un lavoratore nei confronti dell'ex datore di lavoro, lamentando la violazione della disciplina in materia di protezione dei dati personali per avere quest'ultimo attuato un monitoraggio abusivo del traffico in rete (tramite il conteggio del tempo trascorso e l'analisi delle pagine web visitate), a seguito dell'installazione di un sistema di proxy per finalità di contrasto agli attacchi alla rete da parte di hacker. In quella sede, il Garante ha ritenuto il controllo realizzato dal datore di lavoro sul traffico effettuato dal lavoratore sulla rete Internet. Muovendo dal presupposto che le esigenze difensive del datore di lavoro non possono assumere una portata tale da giustificare un totale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore, era evidente che il sistema informatico aziendale, configurato in modo da permettere la registrazione sistematica dei dati concernenti la navigazione web effettuata dalla singola macchina (IP), e quindi dal lavoratore cui la stessa è stata attribuita in via esclusiva, e dunque idoneo a consentire, in ogni momento, l'identificazione del lavoratore stesso utilizzatore della singola macchina, nonché la ricostruzione dell'attività da questo effettuata in rete, non fosse conforme alla disciplina di settore in materia di controlli a distanza (art. 4 St. lav.) né ai principi di necessità,

---

<sup>253</sup> D'ACQUISTO G. - NALDI M., *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017.

<sup>254</sup> Cfr. art. 32 del Regolamento (UE) 2016/679.

<sup>255</sup> Trattamento dei dati personali riferiti alla navigazione internet dei dipendenti - 5 febbraio 2015, in <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3813428>.

pertinenza e non eccedenza dei dati trattati in relazione alle finalità perseguite. Sul tema è di recente intervenuto, con parere dell'8 agosto 2017, il Gruppo di lavoro ex articolo 29 (WP29),<sup>256</sup> il quale ha incoraggiato i datori di lavoro ad adottare specifiche soluzioni volte a prevenire accessi successivi e reiterati ai dati dei lavoratori, presenti, ad esempio, nella loro cronologia web o anche nella casella di posta elettronica, suggerendo, a titolo esemplificativo, misure quali: la previsione di un elenco di siti in cui la navigazione è vietata; la previsione di calendari di posta personali; la predisposizione di un'apposita policy per l'uso della strumentazione informatica.

Sulla base di tali pronunce e pareri, emerge con chiarezza come l'intento, tanto del Garante quanto del WP29, sia quello di guidare e accompagnare il titolare del trattamento (nella specie, il datore di lavoro) nell'adeguamento alle nuove disposizioni europee in materia di tutela della privacy con riguardo al trattamento dei dati personali, indicando misure e strategie concrete idonee a rendere i prodotti e i sistemi conformi ai principi di minimizzazione dei dati, di privacy by design e privacy by default<sup>257</sup>.

Alla luce di quanto detto, tutelare le libertà fondamentali e i diritti dell'utente, anche con riguardo al trattamento dei suoi dati personali, rappresenta una sfida per il futuro, in previsione di un'evoluzione generale e nell'auspicio che l'innovazione tecnologica, di cui si parla e che implica, di riflesso, un rinnovo normativo, sia in grado di offrire all'individuo maggiori sicurezze e tutele, in una società in cui privacy non può essere più il mero "right to be let alone", perché gli interessati sono inevitabilmente immersi in un mondo interconnesso; nella specie la privacy by design sembra essere idonea a offrire un valido strumento per governare questa mole di dati, evitando che dalla loro circolazione e dal loro trattamento possa derivare un eccessivo pregiudizio dei diritti dei singoli.

Si potrebbe pensare alla privacy by design come a un netto *discrimen* tra un passato, caratterizzato da norme generali e astratte poco attente alla tecnologia e alla scienza, e un futuro fatto di norme aderenti a un progresso irrefrenabile e alle esigenze del mondo globalizzato in costante cambiamento. A conferma della fiducia riposta nel principio e nella sua applicazione concreta, si riporta l'affermazione della Dott.ssa Ann Cavoukian, per cui: "*dovesse mai crescere bene nel futuro, la privacy per design garantirebbe il futuro della privacy*"<sup>258</sup>.

---

<sup>256</sup> Il Gruppo di lavoro 29 (Working Party article 29), così definito perché previsto dall'articolo 29 della direttiva europea 95/46, è stato sostituito dall'Edpd (European Data Protection Board o Comitato Europeo per la protezione dei dati) a seguito dell'entrata in vigore del nuovo regolamento europeo.

<sup>257</sup> DE CAROLIS D. - LEONETTI P., *Dalla norma al caso concreto: come la Privacy by Design influenza le dinamiche del rapporto lavorativ*, su <https://www.altalex.com/>.

<sup>258</sup> CAVOUKIAN A., *Privacy by Design*, Ottawa, IPC Publications, 2009.

### 3.3.3 La valutazione d'impatto sui dati personali

Nell'era *ante* GDPR non c'era un'assunzione di responsabilità in prima persona del titolare del trattamento, ma la scelta se intraprendere o meno trattamenti di dati personali potenzialmente rischiosi, frutto di uno studio e di una serie di valutazioni sulla loro pericolosità per la sicurezza del dato e per i diritti e le libertà dell'interessato, era rimessa al Garante privacy. Il titolare, ricevuta l'autorizzazione, non percepiva di aver assunto una diretta responsabilità relativa alla valutazione e successiva attuazione del trattamento, perché questo era a monte stato autorizzato da un altro soggetto, il Garante appunto. L'avvento del Regolamento UE n. 679/2016, con l'art. 35, ha definitivamente incastonato nel quadro normativo europeo lo strumento della valutazione d'impatto sul trattamento dei dati personali, che dona forma concreta al principio di "accountability"<sup>259</sup>.

Coerentemente con il principio di responsabilizzazione, infatti, il nuovo sistema privacy richiede al datore di lavoro, in qualità di titolare del trattamento dei dati, che il controllo a distanza tramite strumenti tecnologici sia preceduto dalla valutazione d'impatto sui dati personali (Data Protection Impact Assessment o DPIA), prescritto come obbligo dall'art. 35 del Regolamento europeo n. 679/2016, ogni volta che il controllo tecnologico da operare risulti essere fonte di rischi potenziali per diritti e libertà dei lavoratori; d'altro canto l'art. 35 del regolamento europeo, obbligando il titolare del trattamento a eseguire una "*valutazione d'impatto sulla protezione dei dati*", ossia una valutazione documentata delle conseguenze negative (impatto) che potrebbero subire i diritti e le libertà fondamentali delle persone fisiche interessate dal trattamento, costituisce la conseguenza dell'approccio basato sul rischio. Il datore di lavoro è così tenuto a mappare ed esaminare periodicamente il rischio che può derivare dai trattamenti e predisporre un documento descrittivo delle principali caratteristiche dei trattamenti, delle misure concretamente intraprese per valutare il rischio d'impatto negativo sugli interessati e degli accorgimenti adottati per contrastarlo<sup>260</sup>.

La DPIA si sostanzia, dunque, in un processo di autovalutazione dal quale deve emergere con precisione l'origine, la natura, la particolarità e la gravità del rischio implicato nell'attività di sorveglianza, nonché le misure apprestate per il suo contrasto<sup>261</sup>.

---

<sup>259</sup> PICA T., *DPIA, quando è obbligatoria e chi sono i soggetti coinvolti*, su <https://www.cybersecurity360.it/>.

<sup>260</sup> INGRAO A., *op. cit.*

<sup>261</sup> L'art. 35, par. 7, GDPR sancisce che "*la valutazione contiene almeno:*

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*
- c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;*
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione."*

L'esito della valutazione risiede poi nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali sia rispettoso del regolamento generale. Testualmente, l'art. 35, comma 3, GDPR stabilisce che *“la valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico”*.

Di solito il potere di controllo a distanza dei lavoratori è esercitato con delle modalità che portano a escludere che il presupposto applicativo della DPIA sia rinvenibile nelle lettere b) o c) dell'art. 35, comma 3, GDPR poiché, in relazione al contesto lavorativo, è improbabile che il trattamento sia configurato su *“larga scala”*<sup>262</sup>. Invece non è raro che il controllo nei luoghi di lavoro sia compiuto tramite il monitoraggio regolare e sistematico delle attività del prestatore di lavoro, anche ai fini di una valutazione qualitativa e quantitativa dell'attività svolta. A titolo esemplificativo, i controlli datoriali effettuati sui terminali elettronici e informativi dei dipendenti, il monitoraggio della navigazione internet e degli account di posta elettronica aziendali, la videosorveglianza e la geolocalizzazione sono tutte attività che richiederanno, se compiute con metodicità, l'adempimento di DPIA<sup>263</sup>.

D'altronde guardando alle ipotesi in cui si richiede al titolare del trattamento la valutazione d'impatto sui dati personali, l'intervento del WP29, cui si attribuisce il merito di aver individuato i nove criteri<sup>264</sup> fondanti il riconoscimento e la qualifica di un trattamento di dati personali “a rischio

---

<sup>262</sup> Il Regolamento non definisce con precisione che cosa si debba intendere per “larga scala”. Il Considerando 91 del Regolamento UE n. 2016/679 ricorda che i trattamenti su larga scala sarebbero quelli che *“mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti”*. Una soluzione interpretativa è stata data anche dal Gruppo di lavoro articolo 29 per la protezione dei dati nelle “linee guida sui responsabili della protezione dei dati” del 5 aprile 2017, WP 243. Secondo il Gruppo per stabilire se un trattamento è stato compiuto su larga scala, bisogna prendere in considerazione una serie di indici, quali il numero di soggetti interessati dal trattamento, il volume dei dati, la durata dell'attività di trattamento e la portata geografica dell'attività del trattamento.

<sup>263</sup> Cfr. VAN DEN HOVEN VAN GENDERN R., *Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics*, in *European Data Protection Law Review*, 2017, III, pp. 338 ss; ROTA A., *Rapporto di lavoro e big data analytics: profili critici e risposte possibili*, in *LLI*, 2017, 3, n. 1, pp. 34 ss.

<sup>264</sup> I nove criteri sono: 1) valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di “aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le

elevato”, desumendo appunto l’obbligatorietà della DPIA, ha permesso la tempestiva adozione, da parte dell’Autorità di controllo italiana e delle autorità degli altri Stati membri, del provvedimento n. 467 recante l’elenco delle tipologie dei trattamenti necessariamente oggetto di valutazione d’impatto<sup>265</sup>. Muovendo dalle linee guida del WP29, secondo cui il ricorrere di almeno due dei nove criteri è indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati e per il quale è quindi richiesta una valutazione d’impatto sulla protezione dei dati, il Garante privacy include tra i trattamenti che devono essere obbligatoriamente sottoposti a DPIA quelli effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti<sup>266</sup>.

Nel caso in cui lo strumento con cui sono stati immagazzinati dati oggetto di trattamento sia stato sottoposto e, all’esperimento della procedura sindacale o amministrativa, con esito positivo, e, a DPIA, è necessario comprendere quale sia il rapporto intercorrente tra i due preventivi adempimenti. In assenza di un’esplicita indicazione, si ammette che l’autonomo esperimento di ciascuna procedura sia legittimo anche perché sono finalizzati ad accertare condizioni di legittimità non equivalenti: l’esperimento della procedura autorizzatoria è volto a verificare l’esistenza delle esigenti richieste dall’art. 4 St. lav.; l’autovalutazione privacy, come ricordato, a individuare i rischi connessi al trattamento dati e le misure per minimizzarli. Data la comunque stretta connessione degli adempimenti, di cui è prova il fatto che l’inadempimento di uno o dell’altro funge da ostacolo

---

preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti dell’interessato”; 2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; 3) monitoraggio sistematico degli interessati; 4) dati sensibili o a carattere altamente personale; 5) trattamento di dati su larga scala; 6) combinazioni di dati; 7) dati relativi a interessati vulnerabili; 8) uso innovativo o applicazione di nuove soluzioni tecnologiche; 9) quando il trattamento “impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto”.

<sup>265</sup> Provvedimento n. 467 dell’11 ottobre 2018, su <https://www.garanteprivacy.it/>.

<sup>266</sup> Gli altri trattamenti sono quelli valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati o lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti dell’interessato; quelli automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi); che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app; i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di miglioramento tecnologico, ecc.; su larga scala di dati aventi carattere estremamente personale, ovvero dati connessi alla vita familiare o privata, o che incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti); trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo); quelli effettuati attraverso l’uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT, sistemi di intelligenza artificiale, monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il Wi-Fi tracking); i trattamenti di categorie particolari di dati ai sensi dell’art. 9 oppure di dati relativi a condanne penali e a reati di cui all’art. 10 interconnessi con altri dati personali raccolti per finalità diverse; quelli sistematici di dati biometrici e genetici.

al trattamento dei dati, si ritiene che sia la DPIA a dover essere effettuata prima della richiesta di autorizzazione all'installazione degli impianti atti al controllo del personale. Le ragioni di tale scelta sono stanzialmente due: in primis perché in fase di DPIA potrebbero riscontrarsi elementi impeditivi del trattamento dei dati, per il cui superamento è richiesta una modifica proprio dei predetti impianti; in secondo luogo in presenza di R.S.A. o R.S.U., il datore di lavoro potrebbe essere spinto da queste ultime a dare conto dell'esito positivo della DPIA durante la trattativa sindacale. In mancanza di rappresentanze sindacali nell'unità produttiva, il datore di lavoro avvierà la procedura amministrativa previa istanza di autorizzazione alla sede territoriale competente dell'INL, al quale, salvo che sia disposto diversamente da specifica disposizione, non è generalmente riconosciuta la possibilità di verificare l'adempimento della DPIA. Nulla vieta al datore di lavoro di procedere successivamente alla valutazione di impatto<sup>267</sup>.

#### **4. Il regime sanzionatorio**

Le modifiche apportate dall'art. 15 lett. f) del d. lgs. n. 101/2018 all'art. 171 del d.lgs. n. 196/2003 si sostanziano in una completa riscrittura di quest'ultimo.

Il novellato art. 171 del d. lgs. n. 196/2003, ora rubricato "*violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori*" in luogo di "*altre fattispecie*" stabilisce che "*la violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge*".

Rispetto alla previgente versione è stata conservata l'impostazione del rinvio legislativo alle sanzioni di cui all'art. 38 St. lav. Quest'ultimo impone la pena dell'ammenda da 154 euro a 1.549 euro o l'arresto da 15 giorni a 1 anno, nell'ipotesi di violazione degli artt. 2, 5, 6 e 15 St. lav.<sup>268</sup>. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente. Quando, per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può supporre inefficace, anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo.

Una lettura della nuova versione dell'articolo in commento consente immediatamente di cogliere le due principali differenze rispetto alla precedente formulazione: la sanzione di cui all'art. 38 St. lav. è ammessa per le violazioni commesse con riferimento al solo comma 1 dell'art. 4 St. lav. ed è

---

<sup>267</sup> RIZZI R. – VENTURA A., *La tutela della privacy del lavoratore controllato a distanza*, in Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili.

<sup>268</sup> Il riferimento alla violazione degli artt. 4 e 8 St. lav. è stato soppresso dall'art. 179, comma 2, d.lgs. 196/2003, disposizione che a sua volta è stata abrogata dall'art. 27, comma 1, lett. c) del d.lgs. 101/2018.

espressamente prevista la medesima sanzione per la violazione delle disposizioni di cui all'art. 8 St. lav, senza rinvio all'art. 113 del d.lgs.196/2003<sup>269</sup>.

Concentrandoci sul primo profilo, rilevante ai fini del presente elaborato, si evidenzia, come chiarito dalla norma con riferimento all'art. 4 St. lav., che saranno penalmente sanzionabili esclusivamente le violazioni relative al primo comma: la fattispecie penale punirà tutte quelle violazioni connesse all'impiego di impianti audiovisivi o altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori per esigenze che non siano organizzative e produttive, legate alla sicurezza sul lavoro o alla tutela del patrimonio aziendale, nonché tutte quelle violazioni legate al mancato rispetto della procedura autorizzatoria (sindacale o amministrativa) per quanto attiene all'installazione degli impianti stessi.

La norma dunque non sanziona più, come in precedenza, le violazioni connesse al secondo comma dell'art. 4 St. lav. e dunque relative ai c.d. strumenti di lavoro e a quelli di registrazione degli accessi e delle presenze. Già sotto la vigenza della precedente versione dell'art. 171 Codice privacy, la dottrina aveva sostenuto che l'unica violazione ipotizzabile dell'art. 4 St. lav. fosse esclusivamente quella relativa al comma 1, dettante le condizioni di installazione e di impiego degli strumenti di potenziale controllo a distanza. Si precisava inoltre come la violazione del comma 1 si concretizzasse anche in tutte quelle ipotesi di errata applicazione del regime del secondo comma a fattispecie invece rientranti nel regime del primo. In linea con tale lettura, in altra sede<sup>270</sup>, era stata messa in luce l'evidente aporia legislativa della precedente versione dell'art. 171 del d.lgs. n. 196/2003 determinata dall'inserimento delle violazioni del secondo comma dell'art. 4 St. lav. nel novero delle condotte penalmente rilevanti. Limitandosi il secondo comma a escludere dalle condizioni di cui al primo i c.d. strumenti di lavoro, si evidenziava come non venisse posto nessun diverso obbligo sanzionabile. Il richiamo del secondo comma, operato dall'art. 171 del Codice privacy, non configurava pertanto la sanzione per una violazione vera e propria giacché la disposizione del comma 2 dell'art. 4 St. lav. non introduceva nessun obbligo, ma comportava esclusivamente un'eccezione rispetto alla disciplina applicabile di cui al comma 1<sup>271</sup>.

Al di là della prospettiva appena delineata, la ragione della modifica legislativa intervenuta potrebbe risiedere nella volontà del Legislatore di sottrarre dal novero delle condotte penalmente sanzionabili

---

<sup>269</sup> La previgente versione dell'art. 171 del d.lgs. 196/2003 disponeva infatti che “*La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300 del 1970*”. Proprio l'art. 113, nella sua precedente formulazione prevedeva che “*Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300*”.

<sup>270</sup> Cfr. PONTI C., *Le fattispecie penali alla luce del novellato Codice Privacy: il quadro*, su <https://www.agendadigitale.eu/>; DAGNINO E., *Tecnologie e controlli a distanza*, in *Diritto delle Relazioni Industriali*, 2015, n. 4, pp. 1004 – 1005.

<sup>271</sup> DAGNINO E., *La Cassazione penale sui controlli a distanza post Jobs Act: continuità del tipo di illecito*, in *Diritto delle Relazioni Industriali*, 2017, n. 1, pp. 181 – 187.

quelle di cui al comma 2 dell'art. 4 St. lav. in virtù di un crescente senso di "liberalizzazione" rispetto a tutti quei c.d. strumenti di lavoro: la novella legislativa quindi terrebbe conto del fatto che, essendo gli strumenti di lavoro dotati di intrinseche potenzialità di controllo, non avrebbe ormai più senso ipotizzare una fattispecie incriminatrice, la quale finirebbe per scontrarsi con un numero di fattispecie quantitativamente sempre maggiore alla luce del costante progresso tecnologico<sup>272</sup>.

L'art. 4, al terzo comma, sancisce, come visto, la regola generale dell'utilizzabilità delle informazioni raccolte ai sensi dei commi precedenti, facendo un ampio riferimento "a tutti i fini connessi al rapporto di lavoro". Tale espressione riveste una rilevanza dal punto di vista processuale in quanto, nelle controversie che insorgono nell'ambito dei rapporti di lavoro, convergono le ipotesi di potenziale illegittimità di raccolta delle informazioni ai sensi dell'art. 4 St. lav.<sup>273</sup>. La generale utilizzabilità di tali dati non è completamente priva di vincoli, in quanto incontra limiti e condizioni normativamente espresse. I dati e le informazioni rilevati a seguito di un controllo a distanza, infatti, sono deducibili in via istruttoria nell'ambito di azioni giudiziarie ma con un limite, ovverosia il rispetto delle condizioni poste a monte, ampiamente descritte in precedenza. Tale non assoluta utilizzabilità si traduce, sul piano processuale, in ipotesi di inutilizzabilità operanti in sede di giudizio e il vincolo giuridico che consente di compiere questa trasposizione è costituito dalla nozione di illiceità della prova.

Le c.d. prove illecite, in cui rientrano i dati e le informazioni illegittimamente acquisite dal datore di lavoro, sono quelle che si sono formate al di fuori del giudizio o acquisite in giudizio "*con mezzi illegali o illegittimi, con metodi penalmente illeciti o con atti che comunque comportino una violazione dei diritti individuali costituzionalmente protetti*"<sup>274</sup>. La conseguenza dell'accoglimento di tale interpretazione a livello processuale è duplice: da un lato, alle parti in giudizio preclude l'ammissione delle prove acquisite in violazione dei vincoli posti dall'art. 4 St. lav.; dall'altro, il giudice non potrà ammetterle in giudizio.

---

<sup>272</sup> PITITTO E.A., *Il "nuovo" art. 171 del Codice Privacy: oltre la razionalizzazione normativa?*, su <http://www.bollettinoadapt.it/>.

<sup>273</sup> GAMBA C., *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove*, in *Labour&Law Issues*, Vol. 2, n° 1, 2016.

<sup>274</sup> Cfr. COMOGLIO P., *Le prove*, Torino, 2010, pp. 51 ss.; INGRAO A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Bari, 2018, secondo cui, ad es., è illecita la raccolta di dati per un diretto scopo disciplinare perché il datore di lavoro per avere un quadro completo dell'efficienza del lavoratore dovrebbe verificarne il comportamento per lunghi periodi di tempo, ma il controllo continuativo è contrario al principio di minimizzazione dei dati che, come visto, stabilisce che il potere di raccogliere dati altrui sia limitato al minimo sia in relazione alla quantità di dati che per il periodo temporale in cui si svolge la raccolta. Giunge dunque ad affermare l'inutilizzabilità dei dati raccolti a tal fine ai sensi del combinato disposto dell'art. 10 del decreto di adeguamento e dell'art. 4, comma 3, St. lav.

## 5. I mezzi di controllo e le nuove tecnologie

La nuova era tecnologica, con i suoi ritrovati sempre all'avanguardia, quali smartphone, droni, dispositivi aziendali, software spia, telefoni attivabili da remoto e strumenti GPS (posizionabili sia sull'autovettura aziendale sia mediante applicazioni su smartphone aziendale), ha tracciato un intricato quadro, con un ampio raggio di controlli, mai sperimentato in precedenza.

A seguito di quest'ondata tecnologica, sono dunque aumentate drasticamente le possibilità concrete di controllo da parte del datore di lavoro. Il Gruppo di lavoro *ex art. 29*, con parere dell'8 giugno 2017, pronunciandosi in merito al trattamento dei dati personali dei lavoratori, anche alla luce del Regolamento (UE) 2016/679, ha tentato di darne una sistemazione individuando vari scenari tipici di controllo e, conseguentemente, di trattamento di dati personali, per lo più basati su un interesse legittimo del titolare del trattamento (datore di lavoro), che possono mettere a rischio i diritti e le libertà dei lavoratori. Per ciascuno di questi scenari, il WP29 ha ricordato che il datore di lavoro, nel rispetto dei principi di *privacy by design* e *privacy by default* previsti dal GDPR e già approfonditi, deve procedere all'individuazione della base giuridica del trattamento, alla verifica della necessità delle operazioni di trattamento e all'esame della correttezza dello stesso rispetto alle finalità perseguite<sup>275</sup>.

### 5.1 Videosorveglianza

Le telecamere di videosorveglianza sono la forma di controllo a distanza più tradizionale, perno della disciplina dettata dall'originario art. 4 St. lav. Tuttavia, negli anni, i sistemi di monitoraggio video sono stati oggetto di un profondo mutamento, occasionato dalla riduzione delle dimensioni delle telecamere e dall'aumento della loro capacità di definizione delle immagini, dall'implementazione di tecniche di analisi delle immagini e dalla cd. videosorveglianza intelligente.

Come ha osservato il Garante per la protezione dei dati personali nel provvedimento a carattere generale del 29 aprile 2004, con riferimento ai rapporti di lavoro *“nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa e ciò anche in caso di erogazione di servizi per via telematica mediante c.d. "web contact center". Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro (art. 4 legge n. 300/1970; art. 2 d.lg. n. 165/2001)”*.

---

<sup>275</sup> AGOSTINI C., *Dati personali dei lavoratori: il WP29 aggiorna le regole del trattamento alla luce delle nuove tecnologie informatiche e del GDPR*, in *Privacy & Data Protection*, 2017.

Tale provvedimento è stato sostituito da un altro provvedimento del Garante in materia di sorveglianza, quello dell'8 aprile 2010, nel quale è prescritto che *“nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge). Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature, "dai quali può derivare 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 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 (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lg. n. 165/2001). Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro, come, ad esempio, nei cantieri edili o con riferimento alle telecamere installate su veicoli adibiti al servizio di linea per il trasporto di persone (artt. 82, 85-87, d.lg. 30 aprile 1992, n. 285, "Nuovo codice della strada") o su veicoli addetti al servizio di noleggio con conducente e servizio di piazza (taxi) per trasporto di persone (le quali non devono riprendere in modo stabile la postazione di guida, e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti, v. punto 4.4.)”*.

Dunque, in ossequio alle norme statutarie, la videosorveglianza rientra nell'area applicativa del divieto assoluto per il caso in cui sia volta a controllare l'adempimento della prestazione del lavoratore, mentre invece rientra in quella del divieto flessibile, superabile con il positivo esperimento della procedura autorizzatoria, quando resa necessaria da esigenze aziendali e quando comporti solo in via riflessa la possibilità di un controllo a distanza<sup>276</sup>.

Proprio perché tale procedura è da osservare, prima che per l'utilizzo dell'impianto, per la sua installazione, va precisato che non è possibile impiantare il sistema di videosorveglianza e mantenerlo spento fino all'ottenimento dell'autorizzazione<sup>277</sup>.

---

<sup>276</sup> Il mancato rispetto della procedura di cui all'art. 4, comma 1, St. lav. espone il datore al ricorso per repressione della condotta antisindacale e all'inutilizzabilità delle immagini in giudizio.

<sup>277</sup> Cfr. BARRACO E. – SITZIA A., *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milanofiori Assago (MI), 2016; GRANDI M., *Impianti di videosorveglianza in ambienti di lavoro. Autorizzazione ad installazione ed uso*, Milanofiori Assago, 2017.

Come visto, l'autorizzazione dell'Ispettorato costituisce una strada sussidiaria rispetto a quella dell'accordo sindacale, operante solo nel caso in cui quest'ultimo non venga raggiunto o in presenza di un'azienda priva di rappresentanze. Qualora, invece, in un'unità produttiva si formino rappresentanze sindacali in precedenza assenti, si può ritenere, che l'autorizzazione eventualmente rilasciata *medio tempore* dall'Ispettorato non sia più sufficiente ai fini del legittimo utilizzo di impianti di videosorveglianza, dovendosi a quel punto tentare la strada dell'accordo, la principale per come designata dall'art. 4 St. lav<sup>278</sup>.

Nel caso in cui, in presenza delle ragioni qualificate, il datore di lavoro avanzi l'istanza con cui richieda l'installazione degli impianti audiovisivi e l'Ispettorato ometta di fornire riscontro all'istante, con la risposta n. 3/2019 all'interpello del Consiglio nazionale dell'ordine dei consulenti del lavoro, il Ministero ha escluso l'assimilazione silenzio-assenso, sottolineando la necessità di un esplicito provvedimento di accoglimento ovvero di rigetto della relativa istanza<sup>279</sup>.

A questa soluzione si è giunti sulla base del fatto che, innanzitutto, con nota del 16 aprile 2012 (prot. n. 7162) il Ministero prende atto, in assenza di specifiche indicazioni circa il rilascio dell'autorizzazione, del consolidamento di una prassi degli organi ispettivi, la quale prevede un sopralluogo preventivo *“per valutare le caratteristiche del sistema e la rispondenza a quanto dichiarato (numero e angoli di ripresa delle videocamere)”*. Il Ministero aveva dunque posto l'accento sulla necessità di considerare i presupposti legittimanti la richiesta di installazione di impianti di controllo, ovvero l'effettiva sussistenza delle esigenze organizzative e produttive, evidenziando inoltre il necessario rispetto del Codice per la privacy, nonché dei successivi provvedimenti del Garante, in particolare delle prescrizioni del richiamato Provvedimento generale sulla videosorveglianza dell'8 aprile 2010, nel quale, tra l'altro, si afferma l'esclusione dell'applicazione del principio del silenzio-assenso in questo caso specifico.

Come si evince dalla nota, tuttavia, il Ministero considera superfluo il sopralluogo per quelle piccole attività, quali ricevitorie, tabaccherie, distributori di carburante ecc.: in tali casi gli organi

---

<sup>278</sup> Nel parere dell'Ispettorato nazionale del lavoro del 24 maggio 2017 si legge: *“La procedura autorizzatoria pubblica, che coinvolge gli Ispettorati del lavoro - territoriali o nazionale - è infatti solo eventuale e successiva al mancato accordo con i sindacati. Tale posizione preferenziale implica, di conseguenza, che anche laddove sia stato rilasciato il provvedimento autorizzatorio per i sistemi di controllo a distanza da parte dell'Ispettorato competente, in seguito a mancato accordo sindacale, l'autorizzazione in parola possa comunque essere sempre sostituita da un successivo accordo”*.

<sup>279</sup> Il Consiglio nazionale dell'ordine dei consulenti del lavoro ha proposto istanza di interpello per conoscere il parere del Ministero del lavoro e delle politiche sociali in merito alla configurabilità della fattispecie del silenzio-assenso con riferimento alla richiesta di autorizzazione all'installazione ed utilizzo degli impianti audiovisivi e degli altri strumenti di cui all'attuale articolo 4, comma 1, della legge 20 maggio 1970, n. 300. E ciò in considerazione delle disposizioni della legge n. 241/1990 che dispongono che il silenzio dell'amministrazione competente equivalga ad accoglimento della domanda.

ispettivi faranno riferimento solo alle specifiche dell'impianto, come il numero e il posizionamento delle telecamere, nonché la planimetria dei locali, risultanti dalla documentazione presentata dal datore di lavoro che diventa parte integrante del provvedimento autorizzatorio<sup>280</sup>.

In secondo luogo, con nota del 18 giugno 2018 (prot. n. 302) in tema di rilascio delle autorizzazioni in esame per esigenze di sicurezza sul lavoro, l'Ispettorato nazionale del lavoro ha altresì ribadito alle proprie strutture territoriali la necessità della stretta connessione teleologica che deve intercorrere tra la richiesta di installazione e l'esigenza manifestata.

In terza battuta, infine, la giurisprudenza, affermando che *“la diseguaglianza di fatto e quindi l'indiscutibile e maggiore forza economico-sociale dell'imprenditore, rispetto a quella del lavoratore, dà conto della ragione per la quale la procedura codeterminativa sia da ritenersi inderogabile, potendo alternativamente essere sostituita dall'autorizzazione della direzione territoriale del lavoro”*<sup>281</sup>, ponendosi così in linea con un orientamento interpretativo consolidato in materia<sup>282</sup>, finisce per condividere la tesi per cui, per come formulato, l'art. 4 St. lav, che esclude solo per gli strumenti menzionati nel secondo comma una necessaria autorizzazione, non ammette la possibilità di installazione e utilizzo degli impianti di controllo in assenza di un atto espresso di autorizzazione, sia esso di carattere negoziale o amministrativo<sup>283</sup>.

A fronte di ciò, ferma la non equiparazione all'assenso del silenzio serbato dall'Ispettorato sull'istanza datoriale di installazione degli impianti audiovisivi, nonchè l'assenza di ogni altra specifica circa la sua interpretazione, e fermo restando, al tempo stesso, che in mancanza di apposita previsione di legge il silenzio non si può leggere come diniego, deve ritenersi che il mancato riscontro alla predetta istanza integri un'ipotesi di silenzio inadempimento, in relazione al quale la legge esclude sì l'operatività del silenzio assenso, ma non definisce l'inerzia come rigetto.

Il Ministero afferma così la necessità che, in caso di istanza ex art. 4 St. lav., l'amministrazione bilanci l'esigenza datoriale e il diritto del lavoratore con il procedimento amministrativo a doversi concludere con un provvedimento espresso ai sensi dell'art. 2 l. n. 241/1990<sup>284</sup>.

---

<sup>280</sup> LEVI A., *Il controllo informatico sull'attività del lavoratore*, Torino, 2013.

<sup>281</sup> Cass., 8 maggio 2017, n. 22148, su <https://www.studiocerbone.com/>.

<sup>282</sup> Si veda Cass., 8 settembre 2016, n.51897, su <https://www.eius.it/>.

<sup>283</sup> Cfr. Interpello n. 3 / 2019; TIRABOSCHI S., *Controllo a distanza e procedimento di autorizzazione amministrativa: i chiarimenti del Ministero del lavoro in ordine al silenzio amministrativo*, su <http://www.bollettinoadapt.it/>.

<sup>284</sup> *“Ove il procedimento consegua obbligatoriamente ad un'istanza, ovvero debba essere iniziato d'ufficio, le pubbliche amministrazioni hanno il dovere di concluderlo mediante l'adozione di un provvedimento espresso. Se ravvisano la manifesta irricevibilità, inammissibilità, improcedibilità o infondatezza della domanda, le pubbliche amministrazioni concludono il procedimento con un provvedimento espresso redatto in forma semplificata, la cui motivazione può consistere in un sintetico riferimento al punto di fatto o di diritto ritenuto risolutivo”*. In caso di inerzia dell'amministrazione pregiudizievole per il datore di lavoro, eventualmente interessato all'installazione di sistemi di videosorveglianza per ragioni organizzativo-aziendali o di sicurezza, data l'impossibilità di tollerare una situazione di limbo permanente, il datore di lavoro potrà rivolgersi al soggetto investito del potere sostitutivo ex art. 2, comma 9- bis, legge n. 241/1990, oppure in caso di inerzia di quest'ultimo potrà rivolgersi al TAR competente per territorio.

L'utilizzazione dei dati acquisiti mediante controllo compiuto con sistemi di rilevazione delle immagini, come risulta dal provvedimento generale 8 aprile 2010, deve avvenire nel rispetto di determinati e precisi principi generali.

In particolare, il trattamento delle informazioni immagazzinate con tali apparecchiature è lecito, oltre che quando l'installazione dei sistemi di videosorveglianza è rispettoso degli oneri procedurali e sussistono le ragioni qualificate, quando è fondato sui principi di necessità e di proporzionalità nella scelta delle modalità di ripresa e dislocazione, nonché di pertinenza e non eccedenza rispetto alle finalità perseguite. Ciò comporta, tra l'altro, un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali, nonché il fatto che l'installazione di sistemi di videosorveglianza per il controllo a distanza dovrebbe essere scelta solo nel caso in cui lo scopo del trattamento non possa essere raggiunto con altri mezzi meno invasivi dei diritti e delle libertà dell'interessato.

La videosorveglianza deve poi avere finalità chiare, prestabilite e legittime: i sistemi di videosorveglianza in azienda hanno la finalità di protezione e incolumità dei dipendenti e di eventuali terzi, di protezione della proprietà e del patrimonio aziendale, di acquisizione delle prove<sup>285</sup>.

Tali principi operano nell'ottica di assicurare una gradualità nell'ampiezza e tipologia di monitoraggio che rende residuali i controlli più invasivi, ammettendoli soltanto se rilevate specifiche anomalie<sup>286</sup>.

Oggi sono diffuse numerose soluzioni di analisi video che consentono l'avvio di funzioni di *motion detection* e *motion tracking*, sistemi software che registrano i movimenti di una persona o di un oggetto nello spazio, o il rilevamento delle espressioni facciali.

La prassi decisoria del Garante italiano e i principali documenti del WP29 hanno confermato un'interpretazione restrittiva della legittimità delle apparecchiature tecnologiche più invasive, a garanzia del lavoratore. In particolare, il Garante ha autorizzato, in un caso di verifica preliminare, l'installazione sul posto di lavoro di un sistema di analisi video in grado di registrare i movimenti delle persone nello spazio, giacché il titolare era in grado di dimostrare l'esistenza di oggettive

---

<sup>285</sup> Cfr. linee guida del Comitato europeo per la protezione dei dati (Ebdp) n.3/19, p.8

<sup>286</sup> Principio espresso dal Garante nel provvedimento dell'8 aprile 2010 e condiviso dall'INL nella circolare n. 5 del 19 febbraio 2018.

esigenze di sicurezza e, in ogni caso, le telecamere potevano essere attivate durante l'orario extra-lavorativo<sup>287</sup>.

Diverso è il discorso per le tecnologie atte a registrare le espressioni facciali per verificare l'eventuale deviazione da modelli standard: l'uso da parte del datore di lavoro non risulta proporzionato al fine da raggiungere<sup>288</sup>. In attuazione del principio di proporzionalità, la conservazione delle immagini registrate da un dato sistema deve essere temporanea, o meglio limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, salvo speciali esigenze per le quali il lasso temporale per la conservazione delle immagini può essere dilatato fino a un massimo di sette giorni<sup>289</sup>. Il sistema impiegato dovrebbe essere programmato in modo che si verifichi, allo scadere del termine previsto, l'automatica cancellazione delle informazioni.

Sempre a tutela del lavoratore, l'elenco di misure minime di sicurezza in materia di videosorveglianza, delineato dal Garante, comprende previsione di vari livelli di visibilità delle immagini, predisposizione delle misure di automatica cancellazione delle registrazioni, accesso limitato ai soggetti in possesso di credenziali di autenticazione abilitanti alla visione delle immagini<sup>290</sup>.

Fra gli obblighi del datore di lavoro espressamente sanciti dal GDPR, risalta quello di fornire ai suoi dipendenti un'adeguata informativa sul trattamento dei dati video e sulle tempistiche di conservazione delle immagini registrate, prima ancora che le telecamere vengano installate e che possano, quindi, riprenderli, anche solo potenzialmente. Inoltre, il datore deve nominare per iscritto, pubblicando i nominativi, i responsabili e gli incaricati del trattamento delle immagini, che devono essere appositamente formati sulle modalità di trattamento dei dati<sup>291</sup>.

È meritevole di maggiore attenzione il principio fondamentale dell'informativa: è necessario che i lavoratori interessati siano sempre informati quando sono in procinto di accedere a una zona video sorvegliata, ossia devono essere consci dell'esistenza e del raggio di azione della videosorveglianza nei luoghi di lavoro dunque monitorati.

---

<sup>287</sup> Sul punto Garante italiano per la protezione dei dati, provvedimento n. 276/2018, Verifica preliminare. Installazione di sistemi di videosorveglianza cd. intelligenti – 9 maggio 2018.

<sup>288</sup> Orientamento condiviso dal Gruppo di lavoro articolo 29, Parere n. 2/2017 dell'8 giugno 2017 in materia di trattamento dei dati sul posto di lavoro.

<sup>289</sup> In merito ai tempi di conservazione delle immagini registrate da certi sistemi, il Garante italiano per la protezione dei dati personali, rispettivamente con i provvedimenti n. 21/2019 e n. 39/2019, sanziona due datori di lavoro che hanno conservato le immagine registrate, senza specifiche esigenze, per 15 e 12 giorni.

<sup>290</sup> RIZZI R. – VENTURA A., op. cit.

<sup>291</sup> ZAMPONI F., *Videosorveglianza sui luoghi di lavoro tra riforme normative e evoluzioni interpretative*, su <https://www.diritto.it/>.

In particolare, nelle linee guida del Comitato europeo per la protezione dei dati (Ebdp) n. 3/19 si legge che i titolari del trattamento dei dati devono operare a più livelli, fornendo in primis l'informativa a livello di segnaletica che, con un'icona grafica visibile, permetta di prendere consapevolezza della videosorveglianza alla quale il luogo è soggetto.

Si tratta di un profilo oggetto di una sentenza della Corte di Cassazione, nella quale si legge che *“l'installazione di un impianto di videosorveglianza all'interno di un esercizio commerciale, costituendo trattamento di dati personali, deve formare oggetto di previa informativa, ex art. 13 del D.Lgs. n. 196 del 2003, resa ai soggetti interessati prima che facciano accesso nell'area videosorvegliata, mediante supporto da collocare perciò fuori del raggio d'azione delle telecamere che consentono la raccolta delle immagini delle persone e danno così inizio al trattamento stesso”*<sup>292</sup>.

La vicenda esaminata dalla Corte parte da un accertamento effettuato dai carabinieri, nel 2009, presso una farmacia dove risultava essere stato installato un sistema di videosorveglianza con immagini riprese in diretta, visibili su un monitor della farmacia e registrate su hard disk non segnalato correttamente: una delle quattro telecamere presenti era infatti posizionata fuori dal negozio mentre l'informativa era presente solamente all'interno della farmacia.

Il Tribunale di Sondrio, in prima istanza, aveva accolto l'opposizione della farmacia, sottolineando che, agli effetti del comma 3 dell'art. 13 del d.lgs. n. 196/2003, il 29 aprile 2004 il Garante aveva adottato un primo provvedimento a carattere generale riguardo all'attività di videosorveglianza, sostituito successivamente con il provvedimento dell'8 aprile 2010. Dunque, all'epoca della contestazione, era ancora in vigore il primo provvedimento adottato dal Garante nel 2004, il quale prescriveva che *“gli interessati devono essere informati che stanno per accedere o che si trovano in zona videosorvegliata”*, mentre solo il provvedimento del 2010 avrebbe prescritto l'onere che l'interessato deve essere *“previamente informato”* che sta per accedere in una zona sorvegliata. Pertanto, per il giudice di merito, avendo i carabinieri comunque accertato la presenza di avviso di zona videosorvegliata all'interno della farmacia, non sussisteva alcuna violazione delle disposizioni del provvedimento del 2004 del Garante.

Il Garante, invece, in sede di ricorso in Cassazione, ha affermato che la soluzione del tribunale contrastava in ogni caso con l'art. 13 del Codice della privacy in tema di informativa, all'epoca non

---

<sup>292</sup> Cass., 5 luglio 2016, n. 13663, su <https://giuricivile.it/>. Con tale sentenza, inoltre, la Suprema Corte ha confermato il suo precedente orientamento. In Cass., 2 settembre 2015, n. 17440, su <https://www.altalex.com/>, infatti si legge, che l'attività di videosorveglianza, pure nell'ipotesi in cui sia svolta in assenza di registrazione, comporta la raccolta ed il trattamento dell'immagine di una persona, che ricade sotto la definizione di *“dato personale”*. Pertanto, sui negozianti che intendano usufruire di sistemi di videosorveglianza, ricade l'onere di rispettare le norme, prescritte dal codice sulla privacy, sull'informativa al cliente che faccia ingresso nel locale.

ancora abrogato, secondo il quale *"l'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto"* del trattamento. La Suprema Corte ha, quindi, accolto le argomentazioni del Garante esprimendo la massima citata poc'anzi<sup>293</sup>.

Potendosi i dispositivi di videosorveglianza trasformarsi in sistemi cd. intelligenti, combinando tra loro ingenti quantità di dati che aumentano il rischio di utilizzi secondari (collegati o meno alle finalità originarie), ovvero di utilizzi illeciti, il Comitato ribadisce, da un lato, che anche nell'utilizzo dei dispositivi video devono essere rispettati i principi applicabili al trattamento di dati personali previsti dal GDPR<sup>294</sup>; dall'altro lato, consente l'impiego della videosorveglianza solo quando non siano rinvenibili altre modalità, meno intrusive, per ottenere il medesimo scopo (cd. "minimizzazione dei dati").

Come anticipato, nelle linee guida n. 3/2019, il Comitato ha rilevato come le finalità di un monitoraggio automatizzato dei luoghi di lavoro mediante dispositivi audiovisivi siano sostanzialmente individuate nella protezione della proprietà, nella tutela della vita e della salute dell'individuo. Tuttavia, com'è pacifico, questa attività comporta la raccolta e la conservazione di immagini e di registrazioni video, ossia di molteplici informazioni delle persone interessate che entrano nel raggio d'azione delle telecamere. Inoltre l'utilizzo di dispositivi intelligenti, come accennato, può ampliare in maniera esponenziale il numero di informazioni e di dati personali raccolti.

Poiché il rischio di utilizzo improprio di questi dati cresce in relazione alla dimensione dello spazio monitorato, nonché in base al numero di interessati potenzialmente coinvolti, il Comitato ritiene necessario procedere con due misure: la valutazione di impatto sulla protezione dei dati (DPIA) e la nomina di un responsabile della protezione dei dati, in base all'art. 37, comma 1, lett. b) GDPR, qualora il trattamento comporti, per sua natura, un controllo regolare e sistematico degli interessati su larga scala.

Tuttavia, il Comitato elenca tre esempi in cui si deroga all'applicazione del GDPR, ossia quei casi in cui un soggetto non può essere identificato direttamente o indirettamente (sfociando, quindi, nella "piena" anonimizzazione): la presenza di telecamere spente, poiché ogni telecamera non funzionante non tratta dati personali, le registrazioni da un'altitudine elevata, come ad esempio mediante droni (il GDPR si applica solo se i dati personali possono essere collegati ad una persona

---

<sup>293</sup> SOFFIENTINI M., *Videosorveglianza sul lavoro e privacy*, Milanofiori Assago (MI), 2018.

<sup>294</sup> Art. 5 GDPR: principi di liceità, correttezza, trasparenza, raccolta per finalità determinate e legittime, adeguatezza, pertinenza, proporzionalità.

specifica); le telecamere da park assist, a condizione che le stesse non raccolgano alcuna informazione relativa a persone fisiche identificate o identificabili (ad esempio targhe)<sup>295</sup>.

Fra i diritti previsti per l'interessato, sono espressamente riconosciuti l'accesso ai dati personali, il diritto di cancellazione e opposizione e il diritto alla trasparenza.

Il Garante per la protezione dei dati personali si è ripetutamente espresso in maniera negativa circa la captazione audio. Pertanto, l'impianto audiovisivo deve essere riferito esclusivamente al sistema video; l'accesso da postazione remota alle immagini "in tempo reale" deve essere autorizzato solo in casi eccezionali debitamente motivati, e quello alle immagini registrate, da remoto e non, deve essere necessariamente tracciato anche tramite apposite funzionalità che consentano la conservazione dei log di accesso per un congruo periodo, non inferiore a sei mesi; infine l'Ispettorato nazionale del lavoro, con circolare n. 5/2018, nel precisare che le eventuali condizioni poste all'utilizzo delle varie strumentazioni utilizzate devono essere correlate alla specifica finalità individuata nell'istanza, afferma che non sussistono particolari e ulteriori limitazioni di carattere tecnico, che talvolta possono rendere vano l'uso dello stesso strumento di controllo. *"L'eventuale ripresa dei lavoratori, di norma, dovrebbe avvenire in via incidentale e con carattere di occasionalità, ma nulla impedisce, se sussistono le ragioni giustificatrici del controllo (ad esempio tutela della "sicurezza del lavoro" o del "patrimonio aziendale"), di inquadrare direttamente l'operatore, senza introdurre condizioni quali, per esempio, "l'angolo di ripresa" della telecamera oppure "l'oscuramento del volto del lavoratore"*.

Se la Suprema Corte sez. III pen., con la sentenza. n. 22611/2012 ricorda che la disposizione di cui all'art. 4 dello Statuto intende tutelare i lavoratori contro forme subdole di accertamento della loro attività da parte del datore di lavoro e che tale rischio viene escluso in presenza di un consenso di organismi di categoria rappresentativi (R.S.U. o commissione interna), *a fortiori*, giunge anche ad affermare che tale consenso deve essere considerato validamente prestato quando arrivi proprio da tutti i dipendenti. L'esistenza di un consenso validamente prestato da parte di chi sia titolare del bene protetto escluderebbe dunque l'integrazione dell'illecito.

Si tratta di una pronuncia isolata che ha, ad ogni modo, rappresentato, per un certo arco temporale, un orientamento che considerava scriminante il consenso prestato dai lavoratori.

La stessa Suprema Corte, con successiva pronuncia<sup>296</sup>, supera la visione del consenso quale unica soglia per ritenere lecita l'installazione di apparecchiature di videosorveglianza, affermando il

---

<sup>295</sup> MISCHITELLI L., *Videosorveglianza e GDPR, i consigli e gli esempi nelle linee guida EDPB*, su <https://www.cybersecurity360.it/>.

principio secondo cui integra reato l'installazione di un sistema di videosorveglianza in grado di controllare a distanza l'attività dei lavoratori, anche quando, in mancanza di accordo con le rappresentanze sindacali aziendali e di provvedimento autorizzativo dell'autorità amministrativa, la stessa sia stata preventivamente autorizzata per iscritto da tutti i dipendenti. D'altronde lo stesso Garante per la protezione dei dati personali ha più volte ritenuto illecito il trattamento dei dati personali mediante sistemi di videosorveglianza, in assenza del rispetto delle garanzie di cui all'art. 4, comma 2, St. lav. e nonostante la sussistenza del consenso dei lavoratori<sup>297</sup>.

Con un cambio di rotta rispetto al passato, è dunque vietato l'uso di apparecchiature di videosorveglianza per il controllo a distanza dei lavoratori ancorché consenzienti.

Occorre preliminarmente un accordo tra datore di lavoro e rappresentanze sindacali. Installare telecamere senza l'interlocuzione con le rappresentanze sindacali "*produce l'oggettiva lesione degli interessi collettivi di cui le rappresentanze sindacali sono portatrici*", in quanto deputate a riscontrare se gli impianti abbiano o meno caratteristiche lesive della dignità dei lavoratori per la loro potenzialità di controllo a distanza, e se siano rispettate le specifiche esigenze organizzative e produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale previste dalla legge.

Il comportamento del datore di lavoro, pertanto, non integra solo una fattispecie di reato penale, ma anche di condotta antisindacale, censurabile con la procedura *ex art. 28* dello Statuto dei lavoratori.

Quanto esposto è stato confermato anche dalle decisioni "gemelle" del 2018: nella prima pronuncia<sup>298</sup>, gli ermellini hanno stabilito che il consenso del lavoratore, prestato in qualsiasi forma (scritta o orale), non vale a scriminare la condotta del datore di lavoro che abbia installato i predetti impianti in violazione delle prescrizioni dettate dalla fattispecie incriminatrice. Per la Corte la *ratio* va rinvenuta nella visione dei lavoratori come soggetti deboli del rapporto di lavoro subordinato.

Con la seconda pronuncia<sup>299</sup>, la Suprema Corte ha precisato che il principio dell'insufficienza del consenso è valido anche se gli strumenti di controllo risultino fuori uso (non funzionanti) o comunque spenti.

In ogni caso se l'azienda, successivamente all'accesso ispettivo, regolarizza la propria posizione mediante la cd. "prescrizione obbligatoria", rimuovendo tutti gli apparecchi non autorizzati, o

---

<sup>296</sup> Cass., 8 maggio 2017, n. 22148, su <https://www.studiocerbone.com/>. Promuoveva infatti ricorso la titolare di un negozio che si era sentita condannare a seguito dell'installazione, all'interno dei luoghi di lavoro un impianto di videoripresa costituito da due telecamere, collegate ad un dispositivo Wi-Fi, ed un monitor, in grado di trasmettere le immagini di ripresa a tale sistema, senza la previa stipulazione di un accordo con le rappresentanze sindacali ed in assenza dell'alternativa autorizzazione della direzione territoriale del lavoro.

<sup>297</sup> Relazione Garante per la protezione dei dati personali, per l'anno 2013, pubblicata nel 2014.

<sup>298</sup> Cass., 24 agosto 2018, n. 38882, su <http://www.lavorosi.it/>.

<sup>299</sup> Cass., 24 agosto 2018, n. 38884, su <https://olympus.uniurb.it/>.

comunque avvia le procedure per la sottoscrizione dell'accordo o richiesta autorizzazione, si estingue il reato anche se già perfezionato.

L'accordo o l'autorizzazione è prescritto anche nel caso in cui l'impianto entri in funzione quando in azienda non sia presente nessuno, al di fuori dell'orario di lavoro, nel caso cioè in cui l'accensione delle telecamere sia collegata al sistema antintrusione.

Difatti, per ledere il bene giuridico protetto della riservatezza dei lavoratori, è sufficiente la mera installazione dell'impianto, anche se questo non è messo in funzione, poiché, configurandosi come un reato di pericolo, la norma sanziona a priori l'installazione, prescindendo dal suo utilizzo o meno<sup>300</sup>. Sulla scia di questa interpretazione, il Ministero del lavoro e delle politiche sociali ha chiarito la possibilità di sanzionare l'azienda anche quando vengano montate, senza le prescritte regole, telecamere "finte", installate al solo scopo dissuasivo<sup>301</sup>.

Infine è opportuno ricordare che il Regolamento (UE) n. 2016/679 sulla protezione dei dati, nella sostanza, non muta il delicato equilibrio raggiunto fra privacy e videosorveglianza.

Il GDPR distingue il trattamento dei dati effettuato con sistema di videosorveglianza a circuito chiuso da quello con immagini inviate a una società che si occupa di videosorveglianza. In quest'ultimo caso, la conformità in materia di privacy (e quindi l'adeguamento per il trattamento e l'utilizzo dei dati) deve essere garantito sia dal soggetto che ha installato il sistema nella propria sede, sia dalla società che riceve le immagini.

## 5.2 Social network

Se, nello scrivere l'art. 4 St. lav., il Legislatore del 1970 aveva come riferimento i sistemi di videosorveglianza, per quanto a un diverso livello di sviluppo, di certo non poteva avere in mente i social network, quali Facebook o Twitter, che hanno ormai travalicato le porte delle fabbriche, degli uffici e in generale dei luoghi di lavoro.

Si tratta di servizi offerti da società operanti su scala mondiale<sup>302</sup> che consentono a ciascun utente, nell'ecosistema cibernetico, di crearsi una vita autonoma, o meglio di ritagliarsi un ruolo nella società digitale, tramite la creazione di un profilo identificativo e l'attiva interazione con gli altri fruitori della rete.

---

<sup>300</sup> Cass., 30 gennaio 2014, n. 4331, su <https://olympus.uniurb.it/>.

<sup>301</sup> SALVI N.M., *Controlli a distanza e consenso dei lavoratori: la Cassazione fa dietrofront*, su <https://www.altalex.com/>.

<sup>302</sup> La direttiva 98/34/CE inquadra i fornitori dei social network a livello giuridico tra i servizi della società di informazione.

Tale situazione è agevolata dalle funzioni tecnologiche che i social mettono a disposizione: supporto per la pubblicazione di immagini, video e commenti, i dati e le informazioni memorizzate nelle reti sociali vanno a costituire una proiezione dei probabili comportamenti dei lavoratori e delle loro caratteristiche personali o professionali, come reputazione o professionalità, potendo fornire precise informazioni non solo in una fase precontrattuale, in sede di assunzione, ma anche durante lo svolgimento del rapporto di lavoro e persino in occasione della sua cessazione, e ancora chat, geo-localizzazione o check-in e individuazione dell'orario in cui ciascuna azione virtuale viene posta in essere e di cui rimane traccia sul supporto digitale, fornito dal provider del servizio. Tracce che per il Legislatore costituiscono dati personali e sensibili, meritevoli di protezione giuridica giacché atti a serbare informazioni potenzialmente lesive della stabilità del rapporto di lavoro<sup>303</sup>.

Queste intrinseche caratteristiche dei social network hanno fatto sì che alla loro originaria funzione di divertimento si affiancasse quella di controllo. Il social network diviene così uno strumento che conferisce al datore di lavoro un potere di controllo a distanza certamente dell'attività dedotta in contratto, ma anche di verifica e investigazione circa la complessiva situazione del dipendente; è una bacheca aperta al pubblico, e quindi anche alla possibile visione da parte del datore di lavoro di quanto "postato"<sup>304</sup>.

A questo punto l'interrogativo che si è posto è capire se il datore di lavoro possa procedere disciplinarmente contro il proprio dipendente una volta rinvenuti *post* che per numero, frequenza e orario d'invio implicino una violazione del dovere di diligenza di cui all'art. 2104 c.c. nell'esecuzione della prestazione lavorativa.

Le prime pronunce giurisprudenziali intervenute in materia hanno ritenuto legittimi i licenziamenti intimati nei confronti dei lavoratori scoperti a chattare su Facebook in orario di lavoro o a condividere espressioni denigratorie nei confronti di superiori gerarchici.

Può citarsi, innanzitutto, l'ordinanza con la quale il Tribunale di Pordenone<sup>305</sup> ha accertato la legittimità del licenziamento imposto al dipendente che aveva condiviso, nella propria bacheca virtuale, pesanti insulti verso il suo responsabile.

Secondo il giudicante, nel caso di specie, l'azienda non aveva violato la normativa sulla privacy, proprio perché la bacheca dei moderni social network rappresenta una "sorta di piazza virtuale" in cui è lo stesso titolare a decidere autonomamente i soggetti con cui interagire. Nel contempo, è stata

---

<sup>303</sup> IAQUINTA F. - INGRAO A., *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, DRI, 2014, 1027.

<sup>304</sup> ROCCHINI E., *Social network e controlli a distanza. Alla ricerca di un difficile equilibrio*, su <http://www.massimariogiurisprudenzadellavoro.it/>.

<sup>305</sup> Trib. di Pordenone ord. 27 giugno 2014, in BARRACO E. – STIZIA A., *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milanofiori Assago (MI), 2016.

esclusa una qualunque violazione dell'art. 4 St. lav. giacché *“la consultazione del social network da parte del Direttore di Stabilimento non è assimilabile ad attività di controllo a distanza mediante apparecchiatura a ciò adibita ex art. 4 St. lav.: l'accesso a Facebook, e in particolare la visualizzazione della bacheca di un “amico” è attività che esula dal contesto lavorativo e che non è in alcun modo configurabile quale attività di controllo remoto”*.

Di maggior interesse, per valutare gli approdi della Corte Suprema è la pronuncia della stessa del 27 maggio 2015 n. 10955<sup>306</sup>, con cui è stato dichiarato legittimo il controllo a distanza, effettuato mediante la creazione di un profilo falso di Facebook per indurre il lavoratore all'attività di chat, quando il controllo è finalizzato all'accertamento di un comportamento lesivo del patrimonio aziendale.

Nella specie, il datore di lavoro, sospettando che il dipendente utilizzasse i social network in orario lavorativo, aveva creato un finto profilo femminile dal quale aveva inviato una richiesta di amicizia al lavoratore, con cui cominciava una fitta chat, in violazione delle disposizioni aziendali che vietavano l'uso del cellulare e lo svolgimento di attività extra-lavorativa in orario di lavoro. Attività pericolosa in quanto, il tempo sottratto all'attività lavorativa si traduce in mancata produttività, elemento caratterizzante l'organizzazione aziendale.

L'interesse della pronuncia in esame risiede nel fatto che i giudici di legittimità, prima di prendere posizione, hanno ricostruito *a priori* i limiti esistenti in materia di controlli. In particolare, la Corte ha affermato che *“sono tendenzialmente ammissibili i controlli difensivi occulti, anche ad opera di personale estraneo all'organizzazione aziendale, in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa, sotto il profilo quantitativo e qualitativo”*.

Tale sentenza, di pochi mesi precedente alla riforma che ha investito l'art. 4 St. lav., è risultata rispettosa anche del nuovo comma 1 della disposizione, che continua a consentire i controlli a distanza solo per fini diversi da quelli immediati di controllo a distanza sull'attività lavorativa dei dipendenti.

Del resto, è stato specificato come la creazione da parte del datore di lavoro di un falso profilo Facebook, attraverso il quale chattare con il lavoratore per verificare l'uso da parte dello stesso del telefono cellulare durante l'orario di lavoro, *“esula dal campo di applicazione dell'art. 4 della legge 20 maggio 1970, n. 300, trattandosi di un'attività di controllo che non ha ad oggetto l'attività lavorativa e il suo esatto adempimento ma l'eventuale perpetrazione di comportamenti illeciti da parte del dipendente idonei a ledere il patrimonio aziendale sotto il profilo del regolare*

---

<sup>306</sup> Cfr, Cass. , 27 maggio 2015, n. 10955, su [www.ilgiuslavorista.it](http://www.ilgiuslavorista.it).

*funzionamento e della sicurezza degli impianti*”: in tal caso il lavoratore era già stato sorpreso al telefono lontano dalla pressa a cui era addetto, che, rimasta incustodita per oltre dieci minuti si era bloccata.

La Corte ha precisato, però, la subordinazione di tale controllo al necessario bilanciamento con i diritti alla dignità e alla riservatezza personale, diritti che tuttavia non sono stati ritenuti superati nel caso in esame: *“resta ferma la necessaria esplicazione dell’attività di accertamento mediante modalità non eccessivamente invasive e rispettose delle garanzie di libertà e dignità dei dipendenti, con le quali l’interesse del datore di lavoro al controllo e alla difesa dell’organizzazione produttiva aziendale deve contemperarsi, e, in ogni caso, sempre secondo i canoni generali della correttezza e buona fede contrattuale”*.

L’utilizzo indebito dei social network può dunque originare responsabilità disciplinare del dipendente che il datore di lavoro è legittimato a far valere senza che venga in rilievo l’art. 4 St. lav., non trattandosi all’evidenza di un controllo a distanza avente ad oggetto l’attività lavorativa dei lavoratori<sup>307</sup>.

Il testo dell’art. 4 St. lav., come riformato dal Jobs Act nel 2015, si articola in un doppio step, come esaminato, la fase dell’installazione delle apparecchiature e quella di utilizzazione dei dati raccolti grazie all’uso delle prime. Per quanto riguarda la fase dell’installazione, la procedura diverge a seconda della natura dello strumento, e dunque, al fine di inquadrare le conseguenze per i social network, bisogna distinguere il caso in cui questi siano strumenti di lavoro e quello in cui, al contrario, siano esclusivamente strumenti di controllo del datore di lavoro.

Il social network, data la sua eclettica polivalenza, rappresenta un paradigma perfetto di come la funzione di lavoro e la funzione di controllo possano condensarsi in un medesimo programma informatico.

Nel caso in cui il lavoratore utilizzi la piattaforma sociale per lavorare, come per coloro che si occupano del c.d. social media marketing, il social ha natura di strumento di lavoro. In tal caso, l’assegnazione delle credenziali (nome utente e password) al dipendente può avvenire senza alcuna formalità e, da quel momento, il lavoratore potrà utilizzare qualsiasi computer per svolgere le sue mansioni, non necessariamente quello aziendale. Il problema, in tali ipotesi, si pone in caso di

---

<sup>307</sup> Cfr. BARRACO E. – SITZIA A., *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milanofiori Assago (MI), 2016; INGRAO A., *Il controllo a distanza realizzato mediante i social network*, vol. 2, no. 1, 2016, p. 105 ss.

patologia nell'utilizzo di uno strumento che, sulla carta, permette un controllo totalizzante<sup>308</sup>. L'art. 4, commi 2 e 3, St. lav. permette al datore di lavoro di acquisire i dati e le informazioni derivanti dall'utilizzo del profilo digitale, al fine di utilizzarli in giudizio, con l'obbligo di rispettare tutti i limiti imposti dalla norma. Si fa riferimento, ovviamente, a tre elementi: l'adeguata informazione che deve essere fornita al lavoratore circa la circostanza che, quando utilizza quello strumento di lavoro, può essere sottoposto a controllo a distanza dal datore di lavoro; il rispetto della normativa in materia di privacy, considerando che le informazioni estrapolate da strumenti tecnologici come i social danno vita a un "trattamento di dati personali", che deve rispondere ai principi di trasparenza, proporzione e prevenzione; il divieto assoluto di controlli prolungati e discriminati, diretta conseguenza del principio di proporzione, per cui è illecito il controllo costante dell'attività del lavoratore in ogni momento in cui è connesso alla rete. Quando queste regole sono violate, i dati acquisiti a seguito di controllo sulle pagine social sono inutilizzabili in un eventuale procedimento disciplinare e nel successivo giudizio<sup>309</sup>.

I limiti di utilizzabilità appena elencati costituiscono la regola generale enunciata dall'art. 4 St. lav. e, dunque, devono essere rispettati anche nell'ipotesi in cui il social network sia utilizzato dal datore di lavoro come vero e proprio strumento di controllo: l'interesse al controllo, come insegna la giurisprudenza, può derivare da input differenti, come anomalie nel funzionamento della rete internet aziendale che spingono il datore di lavoro a un controllo sul numero e sul tempo di connessioni dei dipendenti, piuttosto che la conoscenza di foto o video caricati online dal singolo lavoratore e che risultano sconvenienti per l'immagine del patrimonio aziendale.

Infine, ogni qual volta il datore di lavoro voglia soddisfare l'esigenza di servirsi di strumenti come i social network per controllare eventuali condotte illecite e pregiudizievoli del patrimonio aziendale, deve concludere trattative sindacali dimostrando che lo svolgimento di indagini sui profili dei dipendenti si rende necessario per una delle ragioni che fondano un controllo a distanza legittimo, ad esempio la tutela dei beni immateriali dell'impresa<sup>310</sup>.

### 5.3 BYOD e LOG

In tema di strumenti connessi all'utilizzo della rete digitale, vale la pena soffermarsi su altri due tipi di strumento tecnologico: il *BYOD* e i c.d. *log*.

---

<sup>308</sup> Si fa riferimento al caso in cui, ad esempio, il lavoratore utilizzi il profilo aziendale per svolgere attività estranee rispetto a quelle per cui gli è stato concesso (es. chattare con amici) oppure nell'ipotesi in cui il dipendente manifesti pensieri e opinioni personali non in linea con le strategie e le politiche aziendali.

<sup>309</sup> TESTA D.M., *Il controllo a distanza dei lavoratori ed i Social network*, su <https://www.Jei-JuseInternet.it>.

<sup>310</sup> FAMELI E., *La rilevanza giuslavoristica dei social network, tra diritti dei lavoratori e prerogative datoriali di controllo*, su [www.rivistaitalianadiinformaticadiritto.it](http://www.rivistaitalianadiinformaticadiritto.it).

Il *bring your own device* (c.d. B.Y.O.D.) è un'apparecchiatura tecnologica di recente diffusione e già molto utilizzata, soprattutto all'estero, che permette al dipendente di utilizzare un proprio dispositivo (smartphone, tablet, p.c., ecc.) per connettersi alla rete aziendale e alle sue risorse<sup>311</sup>.

Il BYOD consente di creare, sullo stesso dispositivo (di proprietà del dipendente), due ambienti differenti, contenenti rispettivamente dati personali e dati aziendali, che possono permettere all'utente anche di collegarsi all'intranet aziendale, utilizzandone dati ed applicazioni.

Lo strumento ora sotto esame si caratterizzava per un duplice problema: da un lato, sul piano definitorio e procedurale; dall'altro, in merito alle conseguenze circa la consultazione di dati sensibili e riservati.

In primo luogo, il BYOD ha rappresentato uno strumento di difficile classificazione poiché, pur essendo di proprietà del lavoratore, viene da questi utilizzato avvalendosi di un applicativo di proprietà del datore di lavoro, per accedere a risorse informatiche aziendali<sup>312</sup>. La sua natura "ibrida", pertanto, rendeva complessa l'individuazione del regime di riferimento: la sua appartenenza alla categoria degli strumenti di lavoro, invece che a quella degli strumenti di controllo, lo avrebbe escluso dalle apparecchiature che richiedono l'autorizzazione ai sensi del primo comma dell'art. 4 St. lav.

In secondo luogo, la questione appare ancor più delicata se si considera che l'applicativo BYOD opera sullo strumento di proprietà del dipendente e, dunque, può permettere di assumere informazioni riguardanti non solo l'attività lavorativa, ma dati sensibili del lavoratore stesso che, verosimilmente, essendo il dispositivo di sua proprietà, saranno presenti in modo massiccio.

Il nuovo art. 4 St. lav. non distingue in relazione alla proprietà del dispositivo, includendo nella categoria degli strumenti di lavoro tutti quelli che siano utilizzati dal lavoratore per rendere la prestazione lavorativa. Ne consegue che anche l'applicativo da installare sul dispositivo del lavoratore, purché vi sia il consenso di quest'ultimo, in quanto proprietario dello strumento, e purché sia funzionale allo svolgimento della prestazione lavorativa, può essere annoverato fra gli strumenti di lavoro. La particolare interazione che in questa ipotesi si genera fra lo strumento privato del lavoratore, contenente dati sensibili di quest'ultimo, e la rete aziendale, contenente dati che l'impresa può aver interesse a mantenere riservati, porta a concludere che il datore di lavoro, sebbene non debba ottenere l'autorizzazione all'installazione dello strumento, sarà tenuto ad adottare specifici accorgimenti per assicurare che il monitoraggio dell'attività svolta avvalendosi del BYOD non leda dignità e riservatezza del lavoratore.

---

<sup>311</sup> Per ulteriori approfondimenti tecnici si veda su <https://whatis.techtarget.com/definition/BYOD-bring-your-own-device>.

<sup>312</sup> ALVINO I., op. cit.

Il secondo strumento attinente all'attività digitale che si ritiene meritevole di menzione sono i c.d. log.

Log è un termine usato nell'informatica con diversi significati. Il termine è utilizzato per indicare la registrazione sequenziale e cronologica delle operazioni o effettuate da un utente, da un amministratore, o automatizzate man mano che vengono eseguite dal sistema; il file o insieme di file, su cui tali registrazioni sono memorizzate ed eventualmente accedute in fase di analisi dei dati, è detto anche registro eventi.

Il log più semplice, dalle origini a oggi, è un file sequenziale sempre aperto in scrittura, che viene chiuso e conservato a cadenze regolari e reso disponibile per funzionalità di amministrazione e monitoraggio (logging), quali analisi delle segnalazioni di errore, produzione di statistiche di esercizio, come ad esempio quelle del traffico nei servizi web ripristino di situazioni precedenti, analisi delle modifiche fatte nella base dati, analisi delle operazioni fatte e dei responsabili di tali operazioni, riassunto di quanto successo in un determinato arco di tempo ad esempio nelle chat.

I log, generalizzando, attengono a tutti gli applicativi informatici di ciascuna rete digitale generatrice d'informazioni registrate dal datore di lavoro e, quindi, si prestano anch'essi a una sovrapposizione tra la categoria degli strumenti di controllo e di lavoro. L'analisi della questione, per alcuni punti di vista, appare analoga a quella appena conclusa per il sistema BYOD in quanto, anche per la qualificazione del log, bisogna distinguere tra le due posizioni interpretative tradizionali. Nel caso in cui si accolga la tesi per cui è possibile isolare la composizione dello strumento, e ricavarne da un lato, l'hardware con i suoi applicativi informatici inscindibili, il cui scopo è diretto all'esercizio del lavoro, che non produce log, e, dall'altro, il software volto soddisfare esclusivamente una funzione di controllo, producendo i log, e interfacciandosi con il primo, ma non con la persona che lavora, si potrebbe qualificare il primo come "strumento di lavoro" e il secondo come "strumento di controllo"<sup>313</sup>.

In caso contrario, accogliendo una nozione unitaria di "strumento di lavoro", si finisce per ricomprendervi tutte le funzionalità disponibili sul medesimo hardware e, di conseguenza, i log non sarebbero mai suscettibili di necessaria autorizzazione<sup>314</sup>. In ogni caso, bisogna sempre considerare che l'approccio da utilizzare può variare nel caso concreto e in relazione alla singola novità tecnologica in quanto, riguardo a uno strumento funzionale al lavoro, non è sempre possibile accertare l'autonomia dei programmi informatici installati sullo stesso. Il rovescio della medaglia,

---

<sup>313</sup> MARAZZA M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, CSDLE, Unict, n° 300/2016 su <http://csdle.lex.unict.it/>.

<sup>314</sup> MAIO V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in Arg. Dir. Lav., 2015, I, p. 1186.

pertanto, dal punto di vista pratico, potrebbe essere rappresentato dalle certificazioni di inscindibilità software-hardware che i fornitori di prodotti informatici stilerebbero per i datori di lavoro in relazione agli strumenti assegnati ai dipendenti, quando da questi potrebbero derivare possibilità di controllo<sup>315</sup>.

#### **5.4 Internet e posta elettronica**

Internet e posta elettronica oggi rappresentano strumenti di lavoro pressoché indispensabili, in quanto *“non c’è azienda di qualunque dimensione ed a prescindere dal settore produttivo di appartenenza, non c’è ufficio, non ci sono lavoratori che possano, di fatto, prescindere totalmente nello svolgimento delle loro attività”*<sup>316</sup>.

Anche tali strumenti vanno incontro al divieto di controllo a distanza del lavoratore che, in tale ipotesi, si sostanzia nel divieto di impiego di software al solo scopo di ricostruire le attività svolte dallo stesso. È il caso, ad es., di programmi in grado di leggere e registrare regolarmente i messaggi di posta elettronica, al di là di quanto necessario per svolgere il servizio e-mail, o di software in grado di registrare le pagine web visitate dal prestatore di lavoro.

In relazione ai programmi che permettono controlli indiretti, essi si devono conformare a una logica di graduazione e, sulla base dei principi di trasparenza e correttezza del trattamento dei dati, essere funzionalizzati a prevenire comportamenti non diligenti, e dunque lesivi delle policy aziendali. E il Garante nella prassi decisoria ha proprio battuto sulla prevenzione piuttosto che sulla repressione, sottolineando come l’adozione di policy chiare e trasparenti sia il lascia passare per il corretto trattamento di dati ricavabili dalla posta elettronica e internet in uso al dipendente.

Fermo il divieto per il datore di lavoro di lettura sistematica della posta elettronica e di registrazione metodica delle mail e delle pagine internet lette e visualizzate dal lavoratore, il datore di lavoro può scegliere strumenti e modalità che riducano il più possibile la capacità invasiva delle tecnologie nella sfera di riservatezza del lavoratore.

Tra le *best practice* si ricordano: l’adozione di policy aziendali volte a regolare l’uso di posta elettronica e internet atta a fornire adeguata informazione ai lavoratori circa gli strumenti che consentono il controllo a distanza, le modalità e le regole di utilizzo di tali strumenti; l’individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa,

---

<sup>315</sup> In tale senso MARAZZA M., *Comportamenti illeciti del lavoratore e poteri sanzionatori del datore di lavoro*, in convegno organizzato da Alta Formazione Giuridico-Economia (AGFE), *Privacy e controllo sui lavoratori alla luce dei decreti attuativi dei Jobs Act*, 22 marzo 2016, Roma; BOLOGNINI L., *Utilizzo di strumenti e di tecnologie con finalità di controllo dei lavoratori*, in convegno organizzato da Alta Formazione Giuridico-Economia (AGFE), *Privacy e controllo sui lavoratori alla luce dei decreti attuativi dei Jobs Act*, 22 marzo 2016, Roma.

<sup>316</sup> FOSSATI C. - MORPURGO C., *Internet e azienda*, in Dir. prat. lav., 2001, n. 1, Insetto, III.

misura questa che però ha un risvolto negativo perché, pur consentendo ai lavoratori di conoscere *ex ante* quali siti web sia possibile visitare, con conseguente presunzione di illiceità in caso di rilevamento di navigazione in siti diversi da quelli autorizzati, è nella pratica difficilmente attuabile a fronte della continua emersione di nuovi siti web, che sono ormai milioni. Una schedatura esaustiva degli stessi risulta quasi impossibile; e infine la configurazione di sistemi o l'uso di filtri che prevengano azioni considerate non coerenti con l'attività lavorativa, quali l'upload o l'accesso a certi siti, inclusi in una specie di black list, e il download di file o software aventi determinate caratteristiche, come quelle dimensionali<sup>317</sup>.

Non sembrano esserci dubbi sulla possibilità di qualificare come strumenti di lavoro i computer aziendali e le caselle di posta elettronica, essendo di norma strumenti necessari per lo svolgimento della prestazione lavorativa.

La giurisprudenza infatti è stata chiamata a pronunciarsi sull'applicabilità o meno degli oneri di cui all'art. 4, comma 1, St. lav. in casi di licenziamento di dipendenti motivati dall'uso improprio di pc e posta elettronica emerso a seguito di controlli sugli accessi internet e sulla mail.

Si può pensare al caso dell'impiegata amministrativa alla quale era stato contestato il prolungato uso per fini personali degli strumenti informatici aziendali, uso che era stato causa della contrazione di un virus da parte del sistema informatico della società, che aveva a sua volta comportato la perdita di importanti dati aziendali<sup>318</sup>. In tal caso il giudice di merito ha spiegato che devono considerarsi strumenti di lavoro la posta elettronica e il pc concessi in uso alla dipendente con mansioni d'impiegata amministrativa, in quanto beni necessari all'espletamento dei propri compiti lavorativi. Ne consegue che la loro installazione non richiede gli adempimenti di natura amministrativa e sindacale previsti dall'art. 4, comma 1, St. lav. e che i dati raccolti possono essere utilizzati dal datore ai sensi del comma 3 della stessa disposizione. È possibile dunque per il datore di lavoro controllare l'uso e l'abuso da parte dei dipendenti del pc aziendale, della posta e degli accessi a internet previa informativa ai dipendenti, e nel rispetto dei principi di necessità, pertinenza e non eccedenza, di cui si è ampiamente discusso<sup>319</sup>.

---

<sup>317</sup> Cfr. RIZZI R. – VENTURA A., op. cit., STANCHI A., *Privacy, rapporto di lavoro, monitoraggio degli accessi a Internet, monitoraggio delle e mail, e normative di tutela contro il controllo a distanza. Alcuni spunti per una riflessione interpretativa* in A.A.VV., *I poteri del datore di lavoro nell'impresa*, Padova, 2002, 121; FREDIANI M., *Abuso di accesso ad internet e potere di controllo datoriale*, in *Lav. giur.*, 2002, 947; DELL'ERARIO A. – LOSITO A. – CELIBERTI M., *Controllo a distanza dipendenti: cellulare, tablet, computer aziendali*, su <https://www.theitaliantimes.it/>.

<sup>318</sup> Trib. di Roma, 24 marzo 2017, su <https://www.defensis.it/>.

<sup>319</sup> FALCO W., *Legittimo il controllo sull'uso del pc aziendale e sugli accessi ad internet da parte dei dipendenti*, su <https://www.toffolettodeluca.it/>.

In linea di principio, è riscontrabile pressoché sempre la teorica possibilità tecnologica di far riemergere dalla memoria digitale della macchina (oltre ai computers, anche smart-phones, tablets, fotocamere e videocamere) quei dati che, precedentemente presenti nel supporto di memorizzazione, siano poi stati eliminati<sup>320</sup>.

I dati informatici e digitali, infatti, una volta salvati su files, anche se in seguito cancellati, non vengono mai completamente distrutti: a essere eliminato è il riferimento che punta alla locazione ove il file è conservato, mentre invece, il contenuto dei cluster di dati, corrispondenti ai files, rimane disponibile e recuperabile, fintantoché non sarà sovrascritto.

Il ripristino dei files cancellati e il recupero dei dati sono comunque operazioni complesse e non prive di costi economici per il datore di lavoro, richiedendo il ricorso a opportuni programmi software e a specifiche strumentazioni informatiche, oltre che l'affidamento degli apparati a tecnici specializzati professionisti del settore.

In più, il datore di lavoro può agevolmente accedere alla navigazione internet effettuata dal lavoratore mediante il server aziendale<sup>321</sup>, come pure all'utilizzo della posta elettronica con account aziendale<sup>322</sup>; e al contenuto stesso dei computer aziendali, quando essi sono oggetto di collegamento

---

<sup>320</sup> Dunque, in particolare, l'intero potenziale contenuto dello strumento informatico (computer): i files documentali o recanti immagini, foto, registrazioni audio e video; i messaggi di posta elettronica scaricati, relativi ad account privati; la navigazione internet effettuata mediante una rete di collegamento privata, ossia la cronologia, le pagine visitate (comprese quelle dei motori di ricerca), i downloads effettuati, nonché i dati di login (user ID e password) per l'accesso ad aree riservate dei siti (ad esempio, social networks, internet banking, collegamento skype, ecc.). Il recupero dei dati legati alla navigazione nella rete internet, in particolare, è possibile tramite l'accesso alla cache dei browser internet del PC, che è una porzione di hard disk in cui sono salvate le pagine web visitate, e i relativi contenuti, con la funzione di ridurre il consumo di banda (in quanto, quando si andrà a visitare una seconda volta tali pagine internet, esse verranno recuperate dalla cache senza doverle richiedere e scaricare nuovamente dal server remoto), utilizzando appositi software che permettono di visionare la cache del browser ed estrapolare i dati. Lo stesso vale per i dati tipicamente registrati dagli smartphones: rubrica telefonica; telefonate, sms e mms inviati e ricevuti; foto, video, registrazioni vocali; files; ecc. Al riguardo, bisogna però anche tener conto della maggiore difficoltà di recupero dei dati, nel caso di dispositivi informatici dotati di meccanismi di protezione dell'accesso da parte di terzi (come l'iPhone Apple), o per quelle applicazioni munite di sistemi di criptazione dei contenuti (si veda, ad esempio, l'attivazione della crittografia end-to-end da parte di WhatsApp, per cui i messaggi inviati tramite questa chat e le chiamate non possono essere decodificati neppure dalla società produttrice o gestrice, ma solo dal mittente e dal destinatario).

<sup>321</sup> Specie se l'accesso ad internet avviene attraverso un Proxy cache "http", ovvero un'altra delle possibili funzioni che può svolgere un Firewall. Se la navigazione avviene attraverso il protocollo "http" (HyperText Transfer Protocol), inoltre, chiunque sia in grado di intercettare il traffico internet potrà leggere tutti i dati che transitano tra il PC Client ed il Server Web su cui sono presenti le pagine web. Mentre maggiori garanzie di criptazione e di sicurezza offre la navigazione via "https" (HyperText Transfer Protocol over Secure Socket Layer) (quando è possibile tale tipo di accesso). A meno che, dunque, si utilizzi il protocollo "https" in fase di navigazione, l'amministratore di sistema in possesso delle credenziali di amministratore del Proxy Server potrebbe essere in grado di entrare in possesso persino delle credenziali di accesso (nome-utente e password) inserite nel web browser per l'accesso ad aree riservate dei siti internet. Il recupero successivo del contenuto delle pagine internet visitate mediante il server aziendale è, poi, possibile se il server è configurato per salvare (cachare) la navigazione: in tal caso, oltre alla cache locale del browser internet, vi è anche una cache centralizzata sul Proxy Server.

<sup>322</sup> Con riguardo alla posta elettronica con dominio aziendale, la possibilità di lettura e di conservazione delle mail da parte del Client mail aziendale dipende dal tipo di protocollo utilizzato da quest'ultimo (MUA, Mail User Agent) per recuperare le mail dal Mail Server (MTA, Mail Transfer Agent). I protocolli standard, più utilizzati a tal fine, sono il POP (Post Office Protocol) e l'IMAP (Internet Message Access Protocol). Se il Client utilizza il protocollo POP, le mail

in rete intranet aziendale, con la conseguente condivisione dei contenuti di questi (files e cartelle) e dell'accesso alle stampanti di rete, oltre che ad internet.

In un contesto in cui i pc client accedono alla rete locale e ai servizi da essa offerti, è infatti possibile, da parte dell'amministratore di rete, che verosimilmente sarà in possesso delle password di amministrazione dei client, configurare i pc client in modo che siano raggiungibili e "visionabili" da parte sua. Questi casi sfuggono senz'altro alla possibilità per il lavoratore di limitazione (o di inibizione) del controllo datoriale.

Nelle evenienze prospettate, la possibilità tecnologica di controllo datoriale si scontra, comunque, con le regole dei commi 1 e 2 dell'art. 4 St. lav., vertendo il controllo indiscriminatamente su tutti i contenuti dello strumento informatico (al pari della installazione, da parte del datore, di appositi programmi di monitoraggio in tempo reale delle operazioni effettuate tramite questo): è, pertanto, possibile avanzare dubbi sulla legittimità delle rilevazioni del datore di lavoro.

Particolarmente complicato è, per il datore di lavoro, il recupero dei dati relativi alle operazioni effettuate dal lavoratore mediante lo smartphone, nel caso in cui quest'ultimo sia di proprietà del lavoratore utilizzatore, e quindi non ispezionabile dall'azienda che abbia fornito solo la scheda telefonica (e relativo numero di telefono). In tale ipotesi, il datore di lavoro potrebbe accedere solo ai dati salvati nella sim card (tipicamente, il codice personal identification number- PIN necessario per l'autenticazione in rete del dispositivo cellulare, la rubrica telefonica, i messaggi di testo e la lista delle chiamate); mentre l'acquisizione degli altri dati digitali potrebbe essere tentata solo ricorrendo al gestore telefonico (e all'accesso al traffico transitato attraverso i server di questo).

Ulteriori complicazioni pratiche comporta il controllo datoriale sugli "strumenti misti", ossia in parte di lavoro, in parte di uso personale: ad es., gli abbonamenti telefonici aziendali che prevedono l'utilizzo dell'utenza telefonica anche per telefonate, sms e mms personali (premettendo un determinato codice), con costi a carico dell'utente; o anche i notebook o tablet forniti in dotazione ai lavoratori, o i sistemi di localizzazione satellitare dell'autovettura aziendale, dei quali si consente anche un uso personale. Ciò, per la difficoltà materiale di separare i due tipi di contenuti, personale e aziendale, dello strumento e di accedere solo ai secondi (peraltro, anche ai soli fini della comunicazione del dettaglio di fatturazione da parte del gestore telefonico, nel caso di utilizzo "misto" del recapito telefonico aziendale di rete mobile)<sup>323</sup>.

---

saranno scaricate sul PC Client, che però potrà essere configurato per mantenere una copia delle mail sul server; se, invece, utilizza il protocollo IMAP, le mail presenti sui PC Client saranno sincronizzate con quelle presenti sul server.

<sup>323</sup> TROJSI A., *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, su <http://www.dirittolavorovariazioni.com/>.

## 5.5 Geo-localizzazione

L'utilizzazione di impianti GPS (global positioning system), impianti di localizzazione geografica che consentono al datore di lavoro il monitoraggio dell'esatta posizione dei veicoli aziendali o di altri strumenti elettronici impiegati dal prestatore di lavoro nonché l'identificazione del lavoratore stesso, mediante i dati frutto della geo-localizzazione, rappresenta una delle modalità di controllo a distanza datoriale più discusse in quanto, oltre alle numerose pronunce giurisprudenziali in materia, sia l'Ispettorato nazionale del lavoro che il Garante per la protezione dei dati personali sono intervenuti per delineare delle indicazioni applicative ad hoc<sup>324</sup>.

L'Ispettorato nazionale del lavoro, in data 7 novembre 2016, ha emanato una circolare in materia di installazione e uso di apparecchiature di geo-localizzazione su auto aziendali con una destinazione funzionale: chiarire quando il GPS rappresenti uno strumento di controllo e quando, al contrario, riguardi l'esecuzione della prestazione lavorativa, al fine di individuare i margini applicativi del regime di cui al primo comma dell'art. 4 St. lav.

In linea di principio, l'INL ritiene che i sistemi di geo-localizzazione rappresentino un "*elemento aggiunto agli strumenti di lavoro*", non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa, ma per rispondere a ulteriori esigenze di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro. Per tale motivo, per il loro impiego la regola di carattere generale da seguire è quella dell'accordo sindacale o dell'autorizzazione amministrativa, o in mancanza, dell'autorizzazione dell'INL, ai sensi dell'art. 4, comma 1, St. lav.

L'eccezione, invece, in cui si prescinderebbe da tale regime autorizzatorio, applicando l'art. 4, comma 2, St. lav. è quella in cui i sistemi di geo-localizzazione siano installati per consentire la concreta ed effettiva attuazione della prestazione lavorativa oppure l'installazione sia richiesta da specifiche normative di carattere legislativo o regolamentare (es. uso di sistemi GPS per il trasporto di portavalori superiore a 1.500.000 euro)<sup>325</sup>.

Ogni qual volta che i dati raccolti tramite la geo-localizzazione consentono l'identificazione dei lavoratori dipendenti in via diretta o indiretta, alle imprese si impone il rispetto della normativa privacy.

La prima specifica regolamentazione degli strumenti di localizzazione dei veicoli aziendali risale al provvedimento del 4 ottobre 2011 dell'Autorità Garante per la privacy, che specificava l'obbligo per il datore di lavoro di rispettare il Codice privacy nei casi in cui i dati inerenti l'ubicazione dei

---

<sup>324</sup> SOFFIENTINI M., *Privacy, protezione e trattamenti dei dati*, Milanofiori Assago (MI), 2016.

<sup>325</sup> Cfr. LAMBROU M., *Geolocalizzazione dei veicoli aziendali*, in *Diritto e pratica del lavoro*, 5/2018 p. 297 ss.; DI FRANCESCO M., *Controllo a distanza e utilizzazione di impianti Gps*, *Diritto & Pratica del Lavoro*, n. 10/2017.

veicoli potessero essere associati ai dipendenti, trasformandosi in dati personali. D'altronde la direttiva 2002/58/CE, per come modificata dalla direttiva 2009/136/CE, definisce all'art. 2, lett. c), il dato di ubicazione come "ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico". Siccome il datore di lavoro è sempre in grado di risalire al conducente di un determinato veicolo, è evidente che i dati di localizzazione siano qualificabili come dati personali del lavoratore, la cui gestione configura un'ipotesi di trattamento nel rispetto della normativa privacy.

La disciplina privacy non trova invece applicazione quando le informazioni riguardanti la gestione della flotta aziendale (cd. info – mobilità) sono trattate senza poter essere in alcun modo ricondotte ai lavoratori. Si può pensare alle informazioni relative al consumo del carburante, impiegate solo per la programmazione di una manutenzione efficiente<sup>326</sup>.

Alla luce del d.lgs. 101/2018, l'Autorità Garante è tornata a pronunciarsi sulla questione di geo-localizzazione<sup>327</sup>.

Riprendendo quanto già affermato in passato, è imposto ancora oggi al datore di lavoro il rispetto di determinati principi e l'adozione di misure di sicurezza adeguate ai rischi connessi al trattamento dei dati di geo-localizzazione.

Il Garante specifica che la posizione del veicolo non può essere monitorata costantemente, ma solo quando sia necessario per il conseguimento delle finalità legittimamente perseguite, in ossequio ai principi di necessità di cui all'art. 5, par. 1, lett. c) del Regolamento UE 2016/679.

A tal proposito, l'INL, con nota del 12 novembre 2019 n. 9728, ha dato il via libera ai datori di lavoro per l'installazione di app di geo-localizzazione sullo smartphone concesso in dotazione ai lavoratori addetti alle consegne a due condizioni: che sussistano esigenze organizzative e produttive e che l'app non consenta una geo-localizzazione continua del lavoratore. Quest'ultimo requisito impone quindi che l'app di geo-localizzazione si attivi solo nel momento della consegna della merce, consentendo in tal modo al lavoratore di prendere visione dell'elenco delle consegne giornaliere, di monitorarle in tempo reale, di acquisire prove in caso di controversia con i clienti ecc., o nel caso di richiesta di aiuto da parte del lavoratore, il che rende il sistema di localizzazione utile in relazione alla salute e alla sicurezza sul lavoro, chiudendosi una volta effettuata la richiesta.

---

<sup>326</sup> SOFFIENTINI M., *Geolocalizzazione e impatto privacy*, in *Diritto e pratica del lavoro*, 17/2017 p.889 ss.

<sup>327</sup> Garante per la protezione dei dati personali, provv. 28 giugno 2018 n. 396, doc. web. 9023246; provv. 18 aprile 2018 n. 232, doc. web. 9358266; provv. 24 maggio 2017 n. 247, doc. web. 6495708.

È altresì opportuno che, in base al principio di pertinenza e non eccedenza di cui all'art. 5, par. 1, lett e) GDPR, i tempi di conservazione dei dati medesimi siano commisurati in considerazione degli scopi perseguiti in concreto e che, nel rispetto del principio di minimizzazione dei dati, siano raccolti solo i dati effettivamente utili rispetto agli scopi prefissati dal titolare del trattamento.

Uno dei principali ambiti di applicazione della privacy by design è quello del trattamento di dati personali dei dipendenti effettuato attraverso software di localizzazione installati su dispositivi smartphone o veicoli aziendali.

Già nel 2014, il Garante per la protezione dei dati personali, con provvedimento n. 401 dell'11 settembre 2014, adottato a seguito di una richiesta di verifica preliminare, presentata da una società di telecomunicazioni, a proposito del trattamento di dati personali da compiere tramite l'attivazione di una funzionalità di localizzazione di dispositivi mobili smartphone, forniti in dotazione dalla società ai propri dipendenti, giudicando lecite le finalità perseguite in quanto rispondenti a esigenze organizzative e produttive nonché di sicurezza del lavoro, ritenne il trattamento ammissibile in quanto conforme ai principi di necessità, pertinenza e non eccedenza<sup>328</sup>, precisando, tuttavia, che la società avrebbe dovuto: a) adottare misure e accorgimenti tecnici, ispirati a una logica di privacy by design, idonei a garantire che le informazioni, presenti sul dispositivo mobile, visibili e utilizzabili dall'applicazione installata fossero riferibili soltanto ai dati di geo-localizzazione, nonché a impedire l'eventuale trattamento di dati ultronei (quali quelli relativi al traffico telefonico, agli sms, alla posta elettronica); b) configurare il sistema in modo tale che sul dispositivo fosse posizionata un'icona che indicasse che la funzionalità di localizzazione è attiva; c) consentire l'eventuale trattamento dei dati in tempo reale solo in presenza di specifiche esigenze (ad esempio, legate al verificarsi di situazioni di emergenza e/o di pericolo per il dipendente), individuate all'interno di appositi protocolli; d) consentire l'accesso ai dati trattati ai soli incaricati della società che, in ragione delle mansioni svolte o degli incarichi affidati, potessero prenderne legittimamente conoscenza<sup>329</sup>.

---

<sup>328</sup> A giudizio del Garante le modalità di rilevazione, tali da evitare un monitoraggio continuativo degli spostamenti dei dipendenti, nonché quelle di memorizzazione dei dati, pensate in maniera tale da registrare solo l'ultima informazione relativa alla localizzazione del dispositivo al termine di una determinata sessione di lavoro, procedendo a cancellare automaticamente la rilevazione precedente, rendevano il trattamento complessivamente conforme ai principi di necessità, pertinenza e non eccedenza.

<sup>329</sup> Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a. - 11 settembre 2014, in <https://www.garanteprivacy.it/>.

Di recente, con provvedimento n. 242 del 18 aprile 2018,<sup>330</sup> il Garante è tornato a pronunciarsi in tema di trattamento di dati personali dei dipendenti effettuato a mezzo di sistemi di localizzazione geografica dei dispositivi aziendali, confermando, in buona sostanza, il proprio precedente provvedimento.

Nella specie, il Garante, pronunciandosi in merito a una richiesta di verifica preliminare riguardante il trattamento di dati personali connesso alla prospettata installazione di un applicativo di localizzazione geografica sui dispositivi smartphone o tablet consegnati a guardie giurate, incaricate della vigilanza dei veicoli adibiti a trasporto valori, ha ritenuto il trattamento ammissibile in quanto realizzato con modalità conformi ai principi di necessità, pertinenza e non eccedenza in relazione alle finalità legittimamente perseguite<sup>331</sup>. Nondimeno, il Garante, nell'autorizzare l'installazione dell'applicativo di localizzazione, ha disposto che gli strumenti siano progettati in maniera tale che la configurazione del sistema consenta: a) l'apposizione sul dispositivo di un'icona che indichi che la funzionalità di localizzazione è attiva; b) la disattivazione della funzionalità di localizzazione durante le pause consentite dell'attività lavorativa; c) di oscurare la visibilità della posizione geografica decorso un periodo determinato di inattività dell'operatore sul monitor presente nella centrale operativa relativamente a tale funzionalità.

Accanto a queste misure tecniche, il Garante ha altresì prescritto alla società l'adozione di talune misure organizzative, quali: a) l'individuazione di profili differenziati di autorizzazione relativi alle diverse tipologie di dati e di operazioni eseguibili; b) l'individuazione di tempi di conservazione dei dati in concreto trattati tenendo conto delle finalità perseguite; c) la predisposizione di rapporti per i clienti privi di qualunque riferimento che consenta l'identificazione di dipendenti; d) la designazione quale responsabile esterno del trattamento del fornitore del software di localizzazione; e) la predisposizione di periodiche verifiche di test sulla funzionalità e l'affidabilità dei parametri adottati, in vista della valutazione di eventuali falsi positivi o negativi effettuati dal sistema e la conseguente predisposizione di correttivi a tutela della qualità dei dati trattati.

Dunque in ossequio ai principi di minimizzazione del trattamento e della privacy by default, deve essere configurato un sistema tecnologico in modo tale che siano trattati, per impostazione predefinita, solo i dati strettamente necessari rispetto alla finalità del trattamento, ad es. prevedendo la possibilità di disattivazione della sua funzione durante le pause lavorative consentite, previa comunicazione ai lavoratori o, in alternativa, un sistema di oscuramento della posizione geografica

---

<sup>330</sup> Trattamento di dati personali mediante un sistema di localizzazione geografica dei dispositivi aziendali - 18 aprile 2018, in <https://www.garanteprivacy.it/>.

<sup>331</sup> Nella specie si intende la pseudonimizzazione dei dati delle guardie giurate, accesso in tempo reale ai dati di localizzazione solo al ricorrere di determinate circostanze di necessità ed emergenza e periodizzazione temporale della rilevazione in due minuti.

dei dipendenti, decorso un dato periodo d'inattività dell'operatore, e non dati ulteriori, come può essere l'invio di segnali d'allarme in relazione alla velocità del veicolo. I sistemi di localizzazione dei veicoli impiegati per l'esecuzione di prestazioni lavorative dovranno anche collocare all'interno degli stessi delle vetrofanie recanti l'espressione "veicolo sottoposto a localizzazione". È necessario, infine, come ricordato, nel caso di dispositivi mobili l'apposizione di un'icona indicativa del momento in cui la funzionalità della geo-localizzazione è attiva<sup>332</sup>.

Il datore di lavoro dovrebbe adottare una policy aziendale che specifichi le modalità e le tipologie di controlli effettuabili tramite i dispositivi aziendali geo-localizzati e ai sensi dell'art. 13 GDPR, è obbligatoria l'adeguata informativa ai dipendenti geo-localizzati circa le finalità e le modalità del trattamento dei dati raccolti, e dei tempi di conservazione; il Garante, infine, a conferma dell'estrema attualità e delicatezza della questione, conformemente all'art. 35 GDPR, ha sancito con il provvedimento n. 467 dell'11 ottobre 2018, la doverosità della valutazione di impatto anche per il trattamento dei dati effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici, anche con riguardo ai sistemi di geo-localizzazione<sup>333</sup>.

---

<sup>332</sup> RICCIO R., *La problematica disciplina della geolocalizzazione dei dispositivi aziendali*, su <https://www.cyberlaws.it/>.

<sup>333</sup> BONACOSA P., *Datori di lavoro, nuove regole per effettuare i controlli in linea con la privacy*, in *Privacy – La Nuova disciplina europea*, Guida normativa, Il Sole 24 Ore, febbraio 2018, pp. 114 ss.

## CAPITOLO III

### DALLA NORMA AL CASO CONCRETO

#### 1. Il braccialetto elettronico: la nuova tecnologia made in Amazon

In materia di controllo a distanza, una recente vicenda che ha destato scalpore è quella del braccialetto elettronico, brevettato da Amazon nel gennaio 2018. Si tratta di un “bracciale intelligente” legato al polso dei lavoratori per monitorare la correttezza e la rapidità di ogni singolo movimento e avvisare, con una vibrazione, in caso di errore o ritardo. La notizia, riportata dal sito americano di tecnologia GeekWire, ha in poco tempo suscitato notevole interesse e preoccupazione in quanto, trattandosi di uno strumento che emette impulsi sonori ultrasonici e trasmissioni radio, che consentono all’azienda di capire dove sono le mani del dipendente, e in particolare se si stanno muovendo nel posto “giusto”, con l’invio di segnali aptici, il rischio che la nuova tecnologia si trascina dietro, la causa dell’inquietudine sollevata è l’esponentiale aumento della capacità dell’azienda di controllare i lavoratori.

Nel dibattito che si è acceso in Italia sono diverse le personalità intervenute, spesso a condanna della trovata americana, come il Presidente del Consiglio dei ministri o il presidente della Camera dei deputati allora in carica, rispettivamente Paolo Gentiloni e Laura Boldrini, i quali, sostenitori del lavoro di qualità, e non del lavoro con il braccialetto, di quantità, erano convinti che la creazione di Amazon non fosse altro che una modalità degradante, offensiva della dignità dei lavoratori, giacché sfruttabile per controllarli e sorvegliarli maggiormente. Una certa rilevanza mediatica è stata riscontrata anche a livello europeo, ove è stato più volte marcato il potenziale di tale tecnologia di aumentare la sorveglianza sui lavoratori, fattore che si aggiunge a un ambiente di lavoro già di per sé impegnativo; d’altronde Amazon è spesso stata criticata per le condizioni di lavoro delle persone impiegate nei suoi magazzini, le quali hanno raccontato di essere sottoposte a turni molto serrati e ritmi a volte estenuanti, venendo trasformate in robot umani<sup>334</sup>. Un ex dipendente di Amazon nel Regno Unito ha rivelato, ad esempio, al New York Times, che braccialetti come quelli del brevetto potrebbero sì far risparmiare tempo ai lavoratori, evitando errori inutili, ma che il rischio è comunque che si traducano in un eccessivo controllo sul loro lavoro, peggiorando notevolmente un ambiente lavorativo, come ricordato, già spesso soggetto a polemiche<sup>335</sup>.

---

<sup>334</sup> PARKER C. – VONOWSU B., *AMAZON employees are exposed to such gruelling working conditions, they fall asleep on their feet, it has been claimed*, su <https://www.thesun.co.uk/>.

<sup>335</sup> Cfr. a titolo esemplificativo gli articoli pubblicati sui alcuni giornali europei, consultabili su <https://www.theguardian.com/technology/2018/jan/31/amazonwarehouse-wristband-tracking>, <http://www.handelsblatt.com/unternehmen/handelskonsumgueter/armbaender-fuer-angestellte-amazon-will-jeden-handgriff-seiner-mitarbeiterueberwachen/.html>, <https://www.lesechos.fr/monde/europe/-case-passe-en-europe-en-italie->

Secondo la WIPO (2018), l'organizzazione mondiale per la proprietà intellettuale, uno dei brevetti ottenuti dall'Amazon Technologies, Inc., descrive un meccanismo per il tracciamento e la guida dell'arto di un addetto relativamente alla posizione di un articolo nel deposito. Il braccialetto elettronico, connesso ai database degli inventari e degli ordini, permetterebbe di velocizzare l'attività dei dipendenti mediante la triangolazione immediata dei dati relativi al posizionamento del lavoratore e dei pacchi da ritirare. L'obiettivo dichiarato del braccialetto è quello dunque di perfezionare l'efficienza nel sistema di management dell'inventario, rendendo più facile e rapida la localizzazione degli scaffali dove sono stoccati gli articoli e l'annesso recupero della merce in un ordine: quando verrà effettuato un ordine su Amazon, i dettagli saranno inviati sul mini computer al polso del dipendente che dovrà provvedere istantaneamente a prendere e inscatolare quanto ordinato nel minor tempo possibile, per poi passare al compito successivo. Nel fare ciò, secondo la visuale di Amazon, il lavoratore risulterebbe agevolato dall'avere sempre le mani libere, grazie al posizionamento del braccialetto sul polso. Nel documento, gli ingegneri che hanno sviluppato la nuova tecnologia scrivono che *“i sistemi attuali per tracciare dove sono immagazzinati i prodotti dell'inventario possono richiedere al lavoratore di svolgere atti che gli fanno perdere tempo, per questo sono interessanti tutti i nuovi metodi per tenere traccia di dove sono posizionati prodotti dell'inventario”*. Auspicabilmente *“il tempo misurato e pagato deve essere anche un tempo senza impurità né difetti, un tempo di buona qualità, lungo il quale il corpo resta applicato al suo esercizio. L'esattezza e l'applicazione sono con la regolarità, le virtù fondamentali del tempo disciplinare”*<sup>336</sup>. Facendo leva su queste caratteristiche, l'utilizzo del braccialetto elettronico di Amazon non può considerarsi vietato in quanto finalizzato al controllo dell'attività lavorativa<sup>337</sup>.

Ma il potenziale della trovata dell'e-commerce di Seattle non si arresta qui. Il braccialetto, oltre a rivelare se lo staff sta compiendo i passaggi corretti e più veloci per evadere un ordine, è in grado di geo-localizzare il magazziniere, cd. *picker*, fornendogli il tempo massimo per raggiungere la postazione del prossimo prodotto da prendere sugli scaffali. Se il dipendente impiega più tempo di quello previsto dall'azienda come necessario per spostarsi da una postazione a un'altra, risultando più lento, potrebbe potenzialmente incorrere in una sanzione disciplinare, la cui *ratio* risiederebbe nello scarso rendimento. Tra l'altro, è vero che i lavoratori possono aggiungere nel braccialetto eventuali pause dal lavoro, ma anche in tale ipotesi l'azienda è pronta a intervenire, attribuendo il

---

[levee-de-boucliers-contre-le-bracelet-damazon-.php](http://levee-de-boucliers-contre-le-bracelet-damazon-.php),

[https://www.lanacion.com.ar/-una-pulsera-para-controlar-los-](https://www.lanacion.com.ar/-una-pulsera-para-controlar-los-movimientos-de-lostrabajadores)

<sup>336</sup> FOUCAULT M., *Sorvegliare e punire. Nascita della prigione*, Torino, 1975.

<sup>337</sup> Cfr. ROMANI R., *Braccialetto elettronico e controllo a distanza del lavoratore. Il caso Amazon*, su <https://www.altalex.com>; TEBANO E., *Amazon breveta un braccialetto elettronico che monitora i lavoratori*, su <https://www.corriere.it/>.

tempo massimo della pausa, in base alla ragione per la quale il dipendente la richiede. Il braccialetto elettronico sembra essere uno di quegli strumenti in cui “la tecnologia indirizza, scandisce e registra le singole operazioni, previene errori e difetti, corregge in tempo reale le modalità della prestazione: i lavoratori subordinati possono essere completamente eterodiretti dal sistema intelligente che automatically knows the next step e imposta il compito successivo con ampie capacità predittive, calcolando the operation to ensure quality and control and eliminate manual logging”<sup>338</sup>.

E la domanda diventa dunque legittima: ciò di cui si discute è davvero un mezzo innovativo, volto a ottenere un processo produttivo migliore, come urla a gran voce Amazon, o si tratta di un’arma destinata a deumanizzare il lavoro e schiavizzare sempre di più i lavoratori? Domanda ancor più lecita se si rammenta che già il giornalista francese Jean-Baptiste Malet nel 2013, quando ancora i dipendenti utilizzavano uno scanner palmare per il controllo dell’inventario aziendale<sup>339</sup>, nel suo libro inchiesta<sup>340</sup>, ove racconta la sua esperienza d’infiltrato come lavoratore interinale all’interno di un magazzino francese di Amazon per circa un mese, denunciava, oltre che la pressione alla quale l’azienda sottoponeva i suoi lavoratori<sup>341</sup>, il fatto che “lo sbirro elettronico”, ossia lo scanner-lettore di codici a barre che permetteva di identificare le merci, di cui era dotato ogni dipendente, fosse geo-localizzabile. I capireparto avevano già allora dunque la possibilità di monitorare in tempo reale i dati raccolti dal lettore badge che riguardano tutti i dettagli della prestazione lavorativa di ogni dipendente e sorvegliare il lavoratore stesso, controllandone e, la posizione e, il suo tasso di produttività in tempo reale: lo scanner era dotato di un sistema GPS che controllava spostamenti, velocità dei gesti ed eventuali tempi di pausa<sup>342</sup>. E Malet non è il solo ad aver condotto un’inchiesta simile. Anche Alan Selby, giornalista del quotidiano Mirror, ha indagato dopo una serie di polemiche sulle condizioni di lavoro dei dipendenti Amazon, facendosi assumere dalla multinazionale nel magazzino di Tilbury. Sotto copertura ha documentato ciò che accade all’interno dell’azienda: pause di pochi minuti, obiettivi impossibili da raggiungere, personale sottopagato, rischio di malattie mentali e fisiche, orologi coperti con nastro adesivo per non far vedere allo staff quanto manca al fine turno. “Sono in una gabbia chiusa a chiave (...). Ho nove secondi per afferrare ed elaborare un articolo da spedire per l’imballaggio: ho un obiettivo di 300 articoli

---

<sup>338</sup> TULLINI P. (a cura di), *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell’impresa, in Web e lavoro, Profili evolutivi e di tutela*, Torino, 2017.

<sup>339</sup> Nel magazzino di Amazon, non essendo le merci stoccate in maniera ordinata, per una scelta organizzativa, era stato previsto un sistema informatico idoneo a elaborare dati grazie ai quali ciascun lavoratore può conoscere il luogo di stoccaggio, la disponibilità e le caratteristiche dei prodotti.

<sup>340</sup> MALET J.B., *En Amazonie. Un infiltrato nel “migliore dei mondi”*, Roma, 2013.

<sup>341</sup> L’autore si era unito ai dipendenti Amazon come picker, e, in quanto tale, mai autorizzato a sedersi, era incaricato di recuperare la merce disposta sugli scaffali e di portarla a un collega addetto all’imballaggio.

<sup>342</sup> DE MICCO L., *Schiavitù 2.0: nei magazzini di Amazon mancano solo le frustate*, su <https://www.dagospia.com>.

*all'ora. Mentre mi piego in continuazione sul pavimento, il mio corpo si ribella. Le telecamere controllano ogni mia mossa; lo schermo davanti a me ricorda costantemente le unità da imballare e quanti secondi sto impiegando nel farlo*<sup>343</sup>.

A fronte di ciò l'idea del braccialetto elettronico sembra essere l'ennesimo passo avanti verso un controllo ancora più invasivo dei dipendenti Amazon e non solo.

### **1.1 Il braccialetto elettronico: strumento dal quale deriva anche la possibilità di controllo a distanza o strumento di lavoro?**

All'indomani della notizia del brevetto, l'allora Ministro del lavoro italiano Giuliano Poletti invitava l'azienda al rispetto della legge italiana e ammetteva l'impiego di tali strumenti solo a seguito di un accordo con le rappresentanze sindacali<sup>344</sup>, o in mancanza, di un'autorizzazione dell'INL, finendo così per considerare il dispositivo in esame come uno strumento *“dal quale derivi anche la possibilità del controllo a distanza dei lavoratori”*. In tal modo sembrava aver risolto quell'interrogativo che inevitabilmente si era posto: ossia capire se il braccialetto elettronico fosse definibile come strumento di lavoro, e di conseguenza, capire se rientrasse nel primo o secondo comma dell'art. 4 St. lav. Come affrontato, la risposta a tale quesito dipende da se lo strumento fornito ai dipendenti sia o meno effettivamente indispensabile, necessario per svolgere l'attività lavorativa. Qualora dovesse apparire essenziale all'espletamento delle mansioni, ossia se la capacità tecnica del braccialetto non fosse in grado di individuare il dipendente e di controllarlo nell'attività lavorativa, limitandosi piuttosto ad agevolare e velocizzare la ricerca nel magazzino, al pari degli scanner spesso presenti nei centri di smistamento, non servirebbe il preventivo accordo sindacale o l'autorizzazione dell'Ispettorato<sup>345</sup>.

L'orientamento del Ministro Poletti, che respingeva l'idea dell'indispensabilità del braccialetto elettronico per l'esecuzione dell'attività lavorativa, si basava sulla convinzione che un software come quello prospettato nel caso Amazon, data la sua finalità di efficientamento della produzione, che rappresenta una funzionalità ulteriore rispetto a quella di indicazione dell'ordine e della sua localizzazione, dovesse correttamente essere ricondotto nella categoria di strumenti che, per ragioni organizzative e produttive, consentono anche il controllo a distanza dell'attività dei lavoratori (art. 4, comma 1, St. lav.) con relativa applicazione della procedura e delle esclusive finalità di

---

<sup>343</sup> SELBY A., *Timed toilet breaks, impossible targets and workers falling asleep on feet: Brutal life working in Amazon warehouse*, su <https://www.mirror.co.uk/>.

<sup>344</sup> *“Nel nostro paese c'è una regolazione per legge di tutti gli strumenti che ipoteticamente consentono i controlli a distanza. Se un'azienda intende utilizzare uno strumento con queste caratteristiche deve farlo nel rispetto della legge: ossia avere l'accordo con le organizzazioni sindacali o richiedere l'autorizzazione al ministero”*.

<sup>345</sup> FAVA G., *I braccialetti di Amazon: una possibile nuova forma di controllo dei lavoratori?*, su <https://www.4clegal.com>.

utilizzo<sup>346</sup>. Tuttavia la questione è apparsa più complessa rispetto a com'era stata tracciata dal Ministro e dai sindacati, in quanto, c'era chi sosteneva che il braccialetto elettronico, ancorché macchina potenzialmente capace a raccogliere dati esorbitanti rispetto a quelli utili per il datore di lavoro a misura dell'adempimento della prestazione, per le sue caratteristiche di inoltrare gli ordini dei clienti e di misurare il tempo che il lavoratore impiega per passare da uno scaffale all'altro e prendere l'oggetto da spedire, consente a chi lo indossa di ricevere le direttive e adempiere le sue obbligazioni, anche in modo più celere ed efficiente, a tutto vantaggio dell'imprenditore<sup>347</sup>; diventando in tal modo strumento necessario per l'espletamento delle mansioni. Tenendo a mente ciò e quanto affermato dall'INL nella circolare 2/2016, richiamata nel precedente capitolo, tali braccialetti sembrerebbero avere lo scopo di agevolare l'adempimento della prestazione lavorativa e ciò indurrebbe a inserire il dispositivo elettronico nell'alveo dell'art. 4, comma 2, St. lav.<sup>348</sup>, fermi restando in capo al datore di lavoro e, l'onere di preventiva informazione ai lavoratori circa le modalità di uso del braccialetto e di effettuazione dei controlli, e, l'obbligo di rispettare la normativa sulla privacy, giacché una volta introdotto, non sarà possibile fare del braccialetto e delle sue potenzialità di controllo un uso indiscriminato, essendo imprescindibile il rispetto dei principi di pertinenza, correttezza e non eccedenza del trattamento.

## 1.2 Il braccialetto elettronico e la privacy

Altro nodo da sciogliere è quello inerente i limiti di utilizzabilità delle eventuali informazioni raccolte dall'apparecchiatura. Tuttavia appare pacifico ammettere che, qualora il braccialetto dovesse essere programmato in modo da immagazzinare informazioni ultronee rispetto a un uso lecito, i dati raccolti da Amazon non siano utilizzabili contro il lavoratore proprio perché esorbitanti rispetto allo scopo legittimo, ossia non necessari e finalisticamente inammissibili poiché sfruttati per un fine di controllo non ammesso dall'ordinamento. Infatti, un conto è brevettare uno strumento

---

<sup>346</sup> DAGNINO E., *Il braccialetto di Amazon, facciamo chiarezza*, su <http://www.bollettinoadapt.it/>.

<sup>347</sup> Giampiero Proia, professore ordinario di diritto del lavoro all'università Roma Tre ha sottolineato a Labitalia che "in Italia, ci sono norme che limitano i poteri di controllo dei datori di lavoro mediante strumenti digitali ed elettronici. La legge fa una distinzione fra l'apparecchiatura di controllo esterna allo strumento di lavoro, come una telecamera apposta nell'ambiente di lavoro, e una di controllo inserita dentro lo strumento di lavoro, come potrebbe essere il sistema del Pc o anche il braccialetto di Amazon, che l'azienda intende come strumento per aiutare i lavoratori a orientarsi". "Per le apparecchiature esterne, spiega Proia, c'è bisogno o di un'autorizzazione preventiva o di un accordo sindacale. Nel secondo caso, invece, le norme sono semplificate e questa autorizzazione non serve. E questo potrebbe essere il caso di Amazon. Ma c'è da dire, che permangono comunque limiti nell'utilizzo dei dati ricavati da queste strumentazioni". Il professore ha poi continuato "ammesso e non concesso che questo braccialetto di Amazon sia uno strumento di lavoro, dato in dotazione al dipendente, conclude il professore, le informazioni in possesso del datore di lavoro possono essere usate per contestazioni di tipo comportamentale al lavoratore solo nell'ambito della disciplina sulla privacy".

<sup>348</sup> DI MEO R., *Tecnologie e poteri datoriali: commento a margine del cd. braccialetto Amazon*, in *Labour & Law Issues*, vol. 4, no. 1, 2018, pp. 11-13.

che, al polso dei dipendenti, indichi loro legittimamente dove andare e cosa fare, altro è che lo strumento sia anche in grado di raccogliere informazioni sul lavoratore che esorbitino rispetto a tale scopo e che permetta di controllare a distanza i lavoratori. In questo secondo caso l'utilizzo del braccialetto non è ammissibile per ragioni sistematiche giacché, anche dopo la novella dell'art. 4 St. lav., si deve ritenere, con la prevalente dottrina<sup>349</sup>, che la pura finalità di controllo a distanza dell'attività dei lavoratori non sia un fine lecito per il datore di lavoro, il quale, dunque, per rendere utilizzabili i dati raccolti dal braccialetto dovrebbe dare ai lavoratori, come anticipato, adeguata informazione circa l'utilizzo e, in ogni caso, potrebbe utilizzare tali dati solo nel rispetto di quanto previsto dal Codice della privacy, ai sensi di quanto disposto *ex art.* 4, comma 3, St. lav.

A tal proposito, vengono in soccorso gli interventi del Garante della privacy: in una delle prime deliberazioni del 2007, con oggetto il trattamento dei dati personali raccolti per mezzo di posta elettronica e internet<sup>350</sup>, il Garante ha previsto che nell'esercizio della prerogativa del datore di lavoro di verificare l'adempimento della prestazione lavorativa, *“occorre rispettare la libertà e la dignità dei lavoratori”*; e quindi in applicazione del principio di necessità *“il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (...) e, comunque, a minimizzare l'uso di dati riferibili ai lavoratori.”* Dal punto di vista organizzativo, il datore di lavoro è chiamato a valutare l'impatto che lo strumento di lavoro, con la sua introduzione, provoca sui diritti dei lavoratori, e a configurare lo strumento stesso con filtri che impediscano all'azienda di raccogliere dati non attinenti al fine legittimo. Sotto il profilo della finalità, invece, è forse utile ricordare che il Garante della privacy ha evidenziato che tale principio non richiede solo di raccogliere le informazioni per uno scopo specifico, lecito e determinato, ma anche che esse non possono essere usate per *“trattamenti ulteriori secondo modalità incompatibili con lo scopo suddetto”*<sup>351</sup>. Dunque la gestione dei dati personali è lecita *“se è finalizzata ad assolvere obblighi derivanti dal contratto individuale. Se tali finalità sono lecite, a livello generale, occorre rispettare il principio della compatibilità tra gli scopi perseguiti: lo scopo perseguito in concreto dal datore di lavoro sulla base del trattamento di dati personali non deve infatti essere incompatibile con le finalità per le quali i medesimi sono stati raccolti”*<sup>352</sup>.

Tuttavia, il braccialetto non appare al momento uno strumento di lavoro che possa utilizzarsi limitando l'onere del datore a un'informativa, per quanto dettagliata sia. Alla luce di ciò, Amazon e

---

<sup>349</sup> Cfr. BARBIERI M., *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)* in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017; CARINCI MT., *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017.

<sup>350</sup> Essa ha fatto seguito al parere n. 8/2001 sul trattamento dei dati personali nell'ambito del rapporto di lavoro.

<sup>351</sup> Si legge ancora nel parere n. 8/2001.

<sup>352</sup> Linee guida sul trattamento di dati personali dei lavoratori, su <https://www.garanteprivacy.it/>.

qualunque altro datore di lavoro che intenda utilizzare i dati dei dipendenti deve essere in linea col GDPR: ammesso e non concesso che l'art 4. St. lav. consenta di fatto l'utilizzo di uno strumento di lavoro e di controllo dei lavoratori quale il braccialetto brevettato da Amazon, deve certamente considerarsi che la sua imposizione ai lavoratori onererebbe Amazon, e in generale qualsiasi datore di lavoro, di adeguarsi preventivamente al GDPR. Questo significa prevedere delle precise policy di raccolta e trattamento dei dati monitorati sul lavoratore, il tutto previa autorizzazione dei competenti enti amministrativi e nel rispetto dello Statuto dei lavoratori.

### **Segue. L'avvento dei microchip: dall'americana Three Square Market all'italiana Fincantieri**

Il controllo dei lavoratori ha conosciuto un forte sviluppo anche negli Stati Uniti, dove, nel 2013, un articolo, *"The boss is watching"*, pubblicato sul The Wall Street Journal, riportava una ricerca dell'Aberdeen Group secondo cui circa un terzo delle imprese monitoravano attraverso congegni elettronici i dipendenti chiamati a lavorare all'esterno. Accanto al braccialetto elettronico, si è in particolare discusso della nuova tendenza a impiantare chip dermali sui lavoratori quasi per comodità, senza pensare alle conseguenze.

Il dottor Carl Sanders, ingegnere elettronico dal 1968, è stato il direttore del progetto per lo sviluppo dei microchip sottocutanei. Egli ha diretto un gruppo di cento fra i migliori scienziati del mondo, in uno studio volto a individuare il punto più appropriato per inserire il microchip all'interno del corpo umano, individuato poi sotto i capelli della fronte umana o sulla mano. L'inserimento di microchip nel corpo umano è oggi un'operazione tecnicamente semplicissima, che non richiede più di una ventina di minuti. Essi sono mini congegni elettronici che, con un volume di circa 5 micromillimetri, possono contenere fino a 250.000 dati, sia in entrata che in uscita, vengono attivati mediante impulsi di onde radio a bassa frequenza e la batteria al litio si ricarica automaticamente grazie ai flussi della temperatura corporea. Si tratta innegabilmente di potenziali mezzi di controllo efficientissimi, essendo muniti di antenna, con cui, attraverso satellite, possono localizzare qualsiasi persona alla quale siano stati impiantati. Sono inoltre muniti di un *"trasponder"*, ossia un sistema d'immagazzinamento e lettura d'informazioni che avviene mediante onde come quelle di un controllo remoto. Inoltre, in tempi non sospetti, Sanders aveva anticipato quali sarebbero state le fasi progressive dell'introduzione dei microchip: aveva previsto che all'inizio sarebbe stata facoltativa per poi diventare obbligatoria, contenendo ogni dispositivo l'intera storia di ognuno<sup>353</sup>. Il tempo fino ora gli ha dato ragione.

---

<sup>353</sup> Cfr. LAMENDOLA F., *Controllare le persone, solo fantascienza? Non proprio*, su [www.ariannaeditrice.it](http://www.ariannaeditrice.it); D'ANGELO G., *Carl Sanders: il creatore del microchip sottocutaneo che si pentì della sua invenzione*, su <https://www.sapereundovere.com/>.

Negli ultimi anni, ha destato scalpore la proposta avanzata ai propri dipendenti dai manager della Three Square Market (32 M), società del Wisconsin, fornitrice di distributori automatici self-service per le sale ristoro, di innestare, su base volontaria, dal primo agosto 2017, un microchip di identificazione a radiofrequenza<sup>354</sup> (RFID) in grado di contenere tutte le informazioni utili alla vita in azienda, come password, codici di accesso, autorizzazioni a sbloccare serrature ecc.; Todd Westby, il CEO dell'azienda, durante un'intervista alla CBNC, aveva oltretutto assicurato che i chip sarebbero stati facilmente rimuovibili in pochi secondi, "*proprio come se si stesse prendendo una scheggia dal dito*". Il dispositivo, grande quanto un chicco di riso, è stato impiantato, su base volontaria, tramite una speciale siringa direttamente tra il pollice e l'indice della mano sinistra dei dipendenti aderenti all'iniziativa. Come riferito da Sciencealert, fonte di notizie scientifiche online, la percentuale di chi ha accettato è stata ben superiore alle attese, notevolmente attirata dal dichiarato scopo dei microchip, largamente sottolineato dall'azienda, di semplificazione di azioni svolte quotidianamente fra le mura dell'azienda, come utilizzare la stampante, segnalare l'arrivo in ufficio, registrare la presenza, fare acquisti ai distributori automatici e sbloccare smartphone e pc; il tutto avviene semplicemente alzando una mano verso l'apposito lettore<sup>355</sup>. Senza contare che la proposta di un impianto volontario in sé ha una presa maggiore rispetto a un'imposizione dall'alto. Tuttavia l'iniziativa ha suscitato grande clamore in tutto il mondo, giacché, nonostante l'azienda abbia assicurato che la privacy dei dipendenti non sarebbe venuta meno grazie al modo in cui il chip è stato congegnato, ossia criptato, spoglio della capacità di connettersi a una rete, e privo di segnalatore GPS al suo interno, venendo sfruttata per lo più una tecnologia che accetta connessioni solo a brevissima distanza, nell'ordine di qualche centimetro, i dubbi sulla privacy restano. Questo sia perché il sistema comunque permette a chi lo gestisce di sapere quante volte un dipendente va in

---

<sup>354</sup> Si tratta di una tecnologia per l'identificazione e/o memorizzazione automatica di informazioni inerenti a oggetti o persone (automatic identifying and data capture, AIDC) basata sulla capacità di memorizzazione di dati da parte di particolari etichette elettroniche, chiamate tag, (concettualmente assimilabili a una chiavetta USB) e sulla capacità di queste di rispondere all'interrogazione a distanza da parte di appositi apparati fissi o portatili, chiamati reader o interrogatori. Questa identificazione avviene mediante radiofrequenza, grazie alla quale un reader è in grado di comunicare le informazioni contenute nei tag che sta interrogando. In un certo senso, i dispositivi RFID possono essere quindi assimilabili a sistemi di lettura e/o scrittura senza fili con svariate applicazioni. Le etichette RFID si distinguono poi in passive, attive, semi passive e semi attive. Quelle passive hanno solo un microchip, con identificativo univoco ed eventuale memoria, che è privo di alimentazione elettrica, un'antenna e un materiale che funge da supporto fisico chiamato "substrato". Al passaggio di un lettore che emette un segnale radio a frequenze basse o medie, la radiofrequenza attiva il microchip e gli fornisce l'energia necessaria a rispondere al lettore, ritrasmettendogli un segnale contenente le informazioni memorizzate nel chip. Quelle attive dispongono di una o più antenne per inviare il segnale di lettura e ricevere le risposte anche su frequenze diverse, una batteria di alimentazione e uno o più tag RFID. Quelle semi-passive sono dotate di batteria, usata solo per alimentare il microchip e non per alimentare un trasmettitore, in quanto in trasmissione si comportano come un'etichetta RFID passiva. Quelle semi attive sono dotate di batteria che alimenta il chip e il trasmettitore in cui per risparmiare energia l'etichetta RFID è disattivata e viene attivata tramite un ricevitore con tecnologia dei tag passivi e quindi in assenza di interrogazioni il tag può operare per tempi lunghi.

<sup>355</sup> GILLIES T., *Why most of Three Square Market's employees jumped at the chance to wear a microchip*, su <https://www.cnbc.com/>.

bagno, quante pause caffè fa, ecc. e sia perché a differenza di uno smartphone, dal microchip sottocutaneo è impossibile allontanarsi. Senza contare, che come insegna la storia, anche e soprattutto dell'art. 4 St. lav., tutto può cambiare, e ammesso e non concesso che attualmente questi sistemi siano "chip passivi", dunque innocui finché non interagiscono con un dispositivo di lettura, emettendo frequenze radio riconosciute da altri dispositivi con i quali sono in grado di comunicare, non è difficile ipotizzare un effettivo utilizzo di questi chip con funzionalità aggiuntive in un futuro prossimo, permettendo all'azienda di seguire i dipendenti ovunque, di sapere 24 ore su 24, 7 giorni su 7 dove si trovino<sup>356</sup>. D'altronde, ispirata dai numerosi chip impiantati nei suoi dipendenti, l'azienda stessa, nella figura di Todd Westby, ha rivelato la volontà di sviluppare un chip più avanzato, alimentato dal calore del corpo umano e inclusivo di funzionalità di tracciamento GPS e di un software di riconoscimento vocale, mascherando il tutto sempre sotto il binomio di convenienza e comodità, dunque di miglioramento della qualità di vita<sup>357</sup>; il co-fondatore dell'azienda Patrick McMullan ha infatti aggiunto che non si tratta solo di GPS o di attivazione vocale, ma alla base del rinnovamento di tali microchip vi è una causa degna, consistente anche nella realizzazione e inclusione nei chip di un sistema di monitoraggio dei segni vitali dei dipendenti<sup>358</sup>.

L'iniziativa americana non è isolata perché sono varie le aziende in tutto il mondo che hanno già adottato queste apparecchiature o vi hanno almeno tentato: già approdata, dal 2014, al mondo dei microchip è la svedese Epicenter, azienda impegnata nel settore high tech,<sup>359</sup> e nel 2015, è stata l'italiana Fincantieri, azienda operante nel settore della cantieristica navale, a tentare di introdurre una modalità simile a quella di cui si è argomentato poc'anzi. In merito, nel corso delle trattative per il rinnovo del contratto integrativo, l'azienda avrebbe chiesto di inserire microchip negli scarponi antinfortunistici e negli elmetti degli operai per migliorare l'organizzazione del lavoro e accrescerne la sicurezza, localizzando in qualunque momento e con precisione i dipendenti. I sindacati intervenuti hanno dichiarato inaccettabile la proposta, ritenendo che essa non avrebbe potuto che tradursi in un sistema di totale controllo e schiavismo elettronico sul lavoratore, per quanto Fincantieri, dal suo lato, abbia giustificato la presenza di tecnologie di localizzazione in

---

<sup>356</sup> Cfr. MANTOVANI R., *Impiegati col chip sottopelle*, su <https://www.focus.it/>; PERRUCCHIETTI E., *Tutti controllati col chip sottopelle*, su <https://www.ariannaeditrice.it/>.

<sup>357</sup> AIELLO C., *Wisconsin company known for microchipping employees plans GPS tracking chip for dementia patients*, su <https://www.cnbc.com/>.

<sup>358</sup> STURMAN C., *Three Square Market hopes to use its microchipping technologies for vulnerable patients*, su <https://www.healthcareglobal.com/>.

<sup>359</sup> ARNOLD D.G. – BEAUCHAMP T. L. – BOWIE N. E., *Ethical Theory and Business*, Cambridge, 2020.

questi sistemi con la necessità di intervenire e localizzare il prima possibile il lavoratore in pericolo, per soccorrerlo in caso d'incendio su una nave<sup>360</sup>.

Alla luce di tali esperienze, si può concludere come microchip sottocutanei, piuttosto che inseriti negli scarponi da lavoro o negli elmetti, braccialetti vibranti ai polsi o GPS integrati nelle cinture siano prevalentemente visti come le nuove tecnologie che stanno rendendo o potrebbero rendere, in caso di adozione, il lavoratore sempre più simile a un cyborg sorvegliabile in stile Grande Fratello<sup>361</sup>. D'altronde, a fronte dell'evoluzione alla quale si è assistito dagli anni settanta fino a oggi, non è utopistico immaginare che, in caso di progressivo "chipping" dei lavoratori, la nostra società potrebbe diventare teatro di un controllo che, da capillare e pervasivo qual è già, passerebbe a essere totale, trasformando ognuno in quell'"uomo di vetro", perfettamente rientrante entro i confini di un nuovo Panottico dell'iper-sorveglianza<sup>362</sup>.

## **2. La videosorveglianza alla luce della giurisprudenza CEDU**

Negli ultimi anni anche la Corte europea dei diritti dell'uomo è stata più volte chiamata a pronunciarsi sulla già conosciuta sfida del bilanciamento tra esigenze contrapposte nell'ambito lavorativo, ma in un contesto nuovo, aggravato dalla preponderante affermazione delle nuove tecnologie<sup>363</sup>: i giudici di Strasburgo sono intervenuti per determinare così i limiti e i confini della tutela del diritto del lavoratore alla riservatezza, di fronte all'esigenza di garantire al datore di lavoro l'esercizio del proprio potere di controllo e di gestione efficiente delle attività produttive.

Caratterizzata da decisioni non sempre coerenti e a volte ribaltate dall'intervento della Grande Camera, l'evoluzione della giurisprudenza dei giudici di Strasburgo in questa materia è l'inconfutabile prova dell'attualità e della delicatezza delle questioni analizzate fino ora e del grande rilievo degli interessi e dei diritti in gioco. La ricerca del temperamento del diritto dei dipendenti alla vita privata con quello dei datori alla protezione dei propri beni e della propria organizzazione aziendale risente del peso crescente che assumono le esigenze dell'impresa; al tempo stesso, è sempre più forte in tutti gli ordinamenti il bisogno di tutela del valore della vita

---

<sup>360</sup> CAMPINI N., "No al microchip nello scarpone", operai in sciopero alla Fincantieri, su <https://genova.repubblica.it/>.

<sup>361</sup> EVANGELISTI D., *Jobs Act, l'occhio della Ue su microchip e braccialetti per controllare i lavoratori*, su <https://www.ilfattoquotidiano.it/>

<sup>362</sup> PERRUCCHIETTI E., *Braccialetti elettronici e microchip. Storie di schiavi e di infiltrati in Amazon*, su <https://rivoluzione.unoeditori.com>

<sup>363</sup> Cfr. CICCOTTI F., *Diritto di accesso del datore di lavoro e diritto alla riservatezza del lavoratore*, in *Il Diritto del lavoro*, Vol. 69, Fasc. 2, 1995; BORGHI P. – MIELI G., *La tutela della privacy nel rapporto di lavoro: le interpretazioni del Garante, gli orientamenti della dottrina e della giurisprudenza, le indicazioni operative per le aziende*, Roma, 2000; FERRANTE V., *Controllo sui lavoratori, difesa della loro dignità e potere disciplinare*, in *RIDL*, 1/2011, 73 ss.; SITZIA A., *Il diritto alla privacy nel rapporto di lavoro tra fonti comunitarie e nazionali*, Padova, 2013; TEBANO L., *Tutela della privacy e potere di controllo del datore di lavoro tra l'ordinamento italiano e le fonti europee*, in *Labour&Law Issues*, 2/2017.

privata, dei dati personali e delle condotte connesse alle libertà fondamentali, di fronte a una evoluzione della scienza delle informazioni che rende controllabile la vita umana, attraverso la raccolta, l'incrocio e la trasmissione di innumerevoli dati.

La Grande Camera della Corte EDU si occupa proprio di tale contemperamento con la sentenza del 17 ottobre 2019, ultimo tassello della vicenda *López Ribalda e altri v. Spagna*, sviluppando indirizzi interpretativi già raggiunti nel noto caso *Bărbulescu v. Romania* due anni prima: la Grand Chamber giunge ad affermare, sia pure alla luce delle peculiarità del caso concreto e nel rispetto di determinate condizioni, la compatibilità dei controlli difensivi con il catalogo dei diritti tutelati dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e, segnatamente, la proporzionalità della misura di controllo, nel caso di specie, della videosorveglianza occulta, rispetto al fine di tutelare gli interessi organizzativo-patrimoniali del datore, in presenza del ragionevole sospetto di condotte furtive dei lavoratori<sup>364</sup>. Nell'esaminare la vicenda *López Ribalda e altri v. Spagna*, che è proprio nel contesto appena richiamato che si inserisce, sarà dunque opportuno non prescindere dalla pronuncia *Bărbulescu v. Romania*, decisa dalla Grande Camera nel 2017<sup>365</sup>, punto di arrivo in tema di controllo della corrispondenza elettronica da parte del datore, nonché dalla decisione sul caso *Antović e Mirković v. Montenegro*, sempre in merito alla videosorveglianza<sup>366</sup>: la ragione di ciò risiede nella circostanza che, dalla lettura congiunta di tali sentenze emerge con chiarezza il percorso evolutivo della giurisprudenza della Corte EDU sul tema della tutela della riservatezza dei lavoratori; inoltre i principi e i criteri alla base di tali decisioni sono chiaramente affermati e continuamente ribaditi, in un richiamo costante dei precedenti rilevanti<sup>367</sup>.

## **2.1 Ante López Ribalda e altri v. Spagna: Bărbulescu v. Romania e Antović e Mirković v. Montenegro**

Esaminando in primis la sentenza *Bărbulescu v. Romania*, decisa nel settembre 2017 dalla Grande Camera, e pronunciata a seguito di *referral* avverso la prima decisione della quarta sezione<sup>368</sup>, il caso vedeva come protagonista Bogdan Mihai Bărbulescu, ingegnere rumeno addetto alle vendite

---

<sup>364</sup> CIRIELLO A., *Videosorveglianza "occulta" sul luogo di lavoro: il caso López Ribalda e altri c. Spagna e la giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *Lavoro Diritti Europa*, no. 3/2019, p. 2 ss.

<sup>365</sup> Corte EDU, *Bărbulescu v. Romania*, 5 settembre 2017, Grande Camera, ricorso n. 61496/08, su <https://hudoc.echr.coe.int/>.

<sup>366</sup> Corte EDU, *Antović e Mirković v. Montenegro*, 28 novembre 2017, sez. II, ricorso n. 70838/13, su <https://hudoc.echr.coe.int/>.

<sup>367</sup> FORMICI G., *Lavoratori e tutela della privacy: l'evoluzione della giurisprudenza della Corte europea dei diritti dell'uomo, tra controllo della corrispondenza elettronica e videosorveglianza*, in *Osservatorio Costituzionale*, Fasc. 1/2018.

<sup>368</sup> Corte EDU, *Bărbulescu v. Romania*, 12 gennaio 2016, sez. IV, ricorso n. 61496/08, su <https://hudoc.echr.coe.int/>.

presso una compagnia privata di Bucarest, che aveva creato, su richiesta del datore di lavoro, un account di messaggia istantanea (Yahoo Messenger) per finalità professionali, allo scopo di rispondere alle richieste dei clienti. Tra il 5 e il 13 luglio 2007, le comunicazioni del ricorrente sulla piattaforma Yahoo Messenger venivano registrate dal datore di lavoro, rivelando come le attività del dipendente su internet fossero nettamente superiori rispetto a quelle dei colleghi: solo dopo aver chiesto spiegazioni al lavoratore, che negava l'uso dell'account aziendale per scopi personali, il datore esaminava le 45 pagine di trascrizione dei messaggi registrati in precedenza, rivelatrici della natura personale, in taluni punti intima, di conversazioni tenute dal lavoratore con il fratello e la fidanzata. In conformità a questa documentazione, il datore poneva quindi fine al rapporto lavorativo. Il regolamento aziendale interno, conosciuto dal lavoratore, vietava l'uso per scopi personali di risorse dell'impresa, quali computer, fotocopiatrici, telefoni o fax; nulla invece era disposto circa la possibilità del datore di effettuare controlli o monitorare la corrispondenza dei propri lavoratori, circostanza che ha indotto il lavoratore licenziato a convenire in giudizio il datore di lavoro. Bărbulescu interpellava la Bucharest County Court, per ottenere una dichiarazione d'illegittimità del licenziamento per violazione del diritto alla riservatezza della corrispondenza, tutelato dall'art. 8 CEDU e riconosciuto anche dalla Costituzione rumena. Il giudice di primo grado, così come quello d'appello, si pronunciava in senso sfavorevole per il lavoratore. I giudici nazionali ritenevano dunque legittimo il licenziamento del ricorrente<sup>369</sup>. Quest'ultimo decideva quindi di adire la Corte EDU, per violazione dell'art. 8 della richiamata Convenzione europea dei diritti dell'uomo, disposizione che sancisce il diritto al rispetto della vita privata e familiare: con sentenza del 12 gennaio 2016, la quarta sezione della Corte di Strasburgo confermava la decisione dei giudici interni<sup>370</sup>. La quarta sezione, infatti, ha ritenuto corretta la valutazione svolta dalle corti rumene, le

---

<sup>369</sup> La Corte d'Appello ricostruiva il contenuto della direttiva n. 95/46/CE "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", individuando i criteri di bilanciamento fissati a livello europeo e applicabili al caso in esame: necessità, trasparenza, legittimità dello scopo, proporzionalità e sicurezza. Trasponendoli nel caso di specie però, i giudici nazionali ritenevano sussistente un equo contemperamento tra riservatezza e potere di controllo del datore, volto a una gestione efficiente dell'azienda.

Inoltre, nel settembre 2007, il ricorrente aveva promosso anche una controversia di natura penale, ritenendo sussistente una violazione della segretezza della corrispondenza tutelata anche dal codice penale rumeno. Nel 2012, il Directorate for Investigating Organised Crime and Terrorism (DIICOT) sosteneva che l'azienda convenuta fosse proprietaria di internet e degli strumenti di lavoro e che detenesse quindi il potere di monitorare i propri dipendenti. Il lavoratore decideva di non appellare questa decisione.

<sup>370</sup> Cfr. INGRAO A., *Il "cyberslacking" e i diritti del lavoratore "catturato nella rete informatica". Note critiche a margine della sentenza della Corte Europea dei diritti dell'Uomo, sez. IV, 12 gennaio 2016, n. 61496, Bărbulescu vs. Romania, in attesa della pronuncia della Grande Camera*, op. cit.; BRESCIANI I., *Il potere di controllo del datore di lavoro sulla posta elettronica aziendale del lavoro (nota di commento a CEDU, sez. IV, 12 gennaio 2016, C-61496/08)*, in *Variazioni su temi di Diritto del Lavoro*, su [http://www.dirittolavorovariazioni.com/index.php?option=com\\_content&view=article&id=268&catid=10&Itemid=31](http://www.dirittolavorovariazioni.com/index.php?option=com_content&view=article&id=268&catid=10&Itemid=31); SITZIA A. - PIZZONIA D., *Il controllo del datore di lavoro su internet e posta elettronica: quale riservatezza sul luogo di lavoro?*, in *Nuova Giur. Civ.*, 6/2016, 899; ILIAS VIGLIOTTI G., *Controlli a distanza e tutela della privacy*

quali hanno appunto ritenuto legittima l'attività di controllo svolta dal datore di lavoro, senza fare alcun riferimento al contenuto delle conversazioni trascritte, e, dunque, senza violare la privacy del ricorrente, anche perché l'inclusione della corrispondenza privata nei beni protetti dall'art. 8 CEDU non avrebbe escluso, entro certi limiti, un legittimo esercizio del diritto datoriale di verificare l'operato dei propri dipendenti; concludeva così per una non violazione dell'art. 8 CEDU e dunque per una legittima aderenza dell'attività di controllo datoriale a tale norma, e altresì, alle disposizioni in materia di protezione dei dati personali<sup>371</sup>.

Del caso è stata successivamente investita la Grande Camera, che ha però ribaltato la precedente decisione, adottando un atteggiamento più pragmatico, tenuto conto anche della normativa internazionale e comunitaria in materia. In particolare, per verificare se fosse mancato un equo contemperamento di interessi i giudici hanno fatto riferimento non solo alla risoluzione 45/95 delle Nazioni Unite<sup>372</sup> e alla Convenzione di Strasburgo del 1981<sup>373</sup>, ma soprattutto alla direttiva 95/46/CE<sup>374</sup> sul trattamento dei dati personali, come già visto, abrogata e oggi sostituita dal Regolamento (UE) 2016/679<sup>375</sup>. Più nello specifico la Grande Camera, nel ricostruire i fatti, si è concentrata sull'effettivo riconoscimento del diritto alla riservatezza degli individui, sostenendo che al lavoratore debba riconoscersi il diritto alla privacy. Nel caso in cui la sfera privata risulti destinataria di una limitazione, agli interessati deve essere data una adeguata e puntuale informazione sulle potenziali attività di controllo e monitoraggio<sup>376</sup>. Particolarmente puntuale è inoltre il riferimento al documento di lavoro prodotto dal Gruppo per la tutela dei dati (ex art. 29 della Direttiva) nel quale si evidenzia come *“il semplice fatto che un'attività di controllo e sorveglianza sia funzionale agli interessi del datore di lavoro non può giustificare di per sé qualsiasi intrusione nella privacy del dipendente e che qualsiasi misura di controllo deve soddisfare quattro criteri: trasparenza, necessità, lealtà e proporzionalità”*<sup>377</sup>.

Una determinata attività di controllo e monitoraggio deve essere necessaria e finalizzata al raggiungimento di uno specifico e legittimo obiettivo ed essere, in concreto, svolta mediante attività legittime e proporzionate rispetto all'obiettivo che si vuole raggiungere; qualunque procedura di

---

*del lavoratore: la CEDU conferma le scelte del legislatore interno. Nota a sentenza CEDU, sez. IV, 12 gennaio 2016, n. 61496/08, in Massimario di giurisprudenza del lavoro, 4/2016, 211 ss.*

<sup>371</sup> CARTA C., *Corte europea dei diritti dell'uomo: la Grande Camera torna sul (e difende il) diritto alla privacy del lavoratore*, su <https://www.rivistalabor.it>.

<sup>372</sup> Risoluzione A/RES/45/95 dell'Assemblea Generale delle Nazioni Unite, 14 dicembre 1990.

<sup>373</sup> Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, Strasburgo, 28 gennaio 1981.

<sup>374</sup> 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.

<sup>375</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

<sup>376</sup> F-46/09, V c. Parlamento europeo, 5 luglio 2011.

<sup>377</sup> Corte EDU, *Bărbulescu v. Romania*, IV Sez., cit., par. 47.

monitoraggio deve comunque essere trasparente, ossia pienamente conoscibile dal dipendente nelle sue modalità di esecuzione e sicura per i suoi dati, che non devono essere condivisi con terzi.

Anche in questo caso dunque, come poi in quello López Ribalda, la Grand Chamber perviene a una soluzione opposta a quella della Camera semplice. Se quest'ultima, valorizzando il divieto di uso delle risorse aziendali per scopi personali espressamente contenuto in un regolamento interno noto ai dipendenti, aveva ritenuto legittimo il monitoraggio effettuato dal datore di lavoro sulle comunicazioni elettroniche di un proprio lavoratore e, pertanto, valido il suo successivo licenziamento per violazione della politica aziendale, la Grande Camera, invece, ricondotte le conversazioni che si hanno sul posto di lavoro ai concetti di "vita privata" e "corrispondenza" di cui all'art. 8 CEDU, ha ritenuto di dover prioritariamente salvaguardare la riservatezza dei lavoratori anche in presenza di una specifica policy, nota ai dipendenti, recante l'espresso divieto di uso delle e-mail aziendali per fini personali e ha trovato sproporzionata l'attività di sorveglianza promossa dal datore di lavoro rispetto alla salvaguardia della privacy di cui il lavoratore poteva legittimamente aspettarsi il rispetto.

Indispensabile per la decisione del caso Bărbulescu, così come del caso López Ribalda, si rivela il giudizio di bilanciamento tra il diritto alla riservatezza dei dipendenti, da un lato, e gli interessi al controllo del datore, dall'altro, da compiere alla stregua dei parametri individuati nella sentenza Bărbulescu e traslati, *mutatis mutandis*, nella sentenza López Ribalda<sup>378</sup>: elementi di valutazione sono l'esistenza di una informazione chiara sull'attività di monitoraggio, sulla sua effettiva invasività e sulle conseguenze dell'uso dei dati raccolti, l'esistenza di un valido motivo per compiere un'attività di per sé altamente invasiva, qual è il monitoraggio delle conversazioni, la possibilità di adottare strumenti di controllo meno pregiudizievoli e la predisposizione di meccanismi di salvaguardia della privacy per quanto possibile.

Analizzando il caso di specie alla luce di questi criteri, la Grande Camera ha ritenuto che le corti nazionali non avrebbero tutelato adeguatamente il diritto alla privacy del dipendente, poiché sarebbe mancato, nei vari gradi di giudizio, l'equilibrato bilanciamento di cui si discute e ha dunque ravvisato una violazione dell'art. 8 CEDU, ritenendo insufficiente la protezione accordata dalle autorità nazionali sotto due profili: in primis la sfera privata del ricorrente è stata fatta oggetto di un'attività di controllo eseguita con modalità ed estensione poco chiare, se non addirittura sconosciute, in dettaglio, al ricorrente; in secondo luogo la mancanza di trasparenza ha comportato un'azione del datore di lavoro del tutto sproporzionata, priva di un reale obiettivo e di una qualche

---

<sup>378</sup> Cfr. CIRIELLO A., op.cit.; BUFFA F., *Il controllo datoriale delle comunicazioni elettroniche del lavoratore dopo la sentenza Bărbulescu 2 della Cedu*, in *Questione giustizia - Osservatorio internazionale*, <http://questionegiustizia.it/articolo/>.

concreta ragione legittimante l'inferenza. Nel ravvisare violazione dell'art. 8 CEDU, la Grand Chamber ha invitato le corti nazionali al rispetto di specifici criteri che, riprendono anche i principi di cui all'art. 5 del Regolamento UE 2016/679, sono utili a determinare la legittimità del controllo datoriale<sup>379</sup>.

Quest'ultimo orientamento della Corte EDU è stato, invero, parzialmente anticipato dal giudice Pinto de Albuquerque: nell'opinione rilasciata in calce alla sentenza della sez. IV, il giudice ha riconosciuto l'accesso a Internet e la privacy sul web come un vero e proprio diritto umano e, come tale, meritevole di tutela ai sensi della Convenzione, eccependo non solo l'assoluta illegittimità della condotta del datore di lavoro, ma evidenziando anche come i lavoratori non abbandonino il diritto alla privacy e alla protezione dei dati ogni mattina davanti alle porte del luogo di lavoro<sup>380</sup>.

È ora interessante richiamare la pronuncia che la sentenza López Ribalda seguirà a stretto giro, ossia la sentenza Antović e Mirković v. Montenegro del 18 novembre 2017<sup>381</sup>. In questo caso, due professori universitari lamentavano che costituisse un'indebita violazione del loro diritto alla privacy la decisione, presa unilateralmente dal preside della facoltà della School of Mathematics dell'università del Montenegro, di installare videocamere di sorveglianza nelle aule d'insegnamento per tutelare l'incolumità delle persone e il patrimonio dell'università. I dati raccolti dalle telecamere venivano protetti da un codice, di cui solo il preside era in possesso, e conservati per un periodo massimo di un anno; di questa decisione era stata comunque data comunicazione ai lavoratori in occasione di un consiglio universitario.

Questa situazione era stata denunciata alla Personal Data Protection Agency montenegrina, ritenendo la videosorveglianza illegittima e immotivata, dal momento che i luoghi in cui venivano tenute le lezioni erano sempre chiusi a chiave prima e dopo le lezioni stesse e gli unici beni presenti erano banchi, sedie e cattedre. I ricorrenti, a seguito di una prima decisione a loro sfavorevole dell'Agency, proponevano impugnazione innanzi all'Agency's Council, smentendo gli esiti delle indagini e sostenendo che telecamere poste all'entrata e all'uscita costituissero già mezzi sufficienti e meno invasivi per garantire la sicurezza dei locali. Il Council ribaltava la precedente decisione, ordinando all'università la rimozione delle telecamere, poiché installate in violazione della normativa nazionale in materia di protezione dei dati.

---

<sup>379</sup> LORÈ F., *La tutela della privacy nell'esercizio del potere datoriale*, fascicolo n. 1/2020, su [www.amministrativamente.com](http://www.amministrativamente.com)

<sup>380</sup> Corte EDU, Bărbulescu v. Romania, 12 gennaio 2016, sez. IV, ricorso n. 61496/08, opinione parzialmente dissenziente del giudice Pinto de Albuquerque, "*workers do not abandon their right to privacy and data protection every morning at the doors of the workplace*", su <https://hudoc.echr.coe.int/>.

<sup>381</sup> Corte EDU, Antović e Mirković v. Montenegro, 28 novembre 2017, sez. II, ricorso n. 70838/13, su <https://hudoc.echr.coe.int/>.

I due professori, a seguito della rimozione, davano avvio comunque a una causa civile contro l'università, l'Agency stessa e lo Stato del Montenegro, al fine di ottenere il risarcimento dei danni subiti a causa della violazione della propria vita privata. La richiesta dei lavoratori veniva però rigettata tanto dalla corte di prima istanza quanto, in secondo grado, dalla Alta Corte. Le corti domestiche rigettavano ogni domanda risarcitoria affermando il principio secondo cui, non può porsi un problema di tutela della vita privata in relazione a condotte poste in essere in luogo pubblico<sup>382</sup>.

I due professori quindi portavano la causa innanzi alla Corte EDU per violazione dell'art. 8 della Convenzione. La Corte EDU, pronunciandosi sul ricorso, ha voluto demarcare i limiti dell'ambito applicativo dell'art. 8 CEDU, sottolineando che la mera circostanza che la prestazione lavorativa, l'insegnamento in questo caso, abbia svolgimento in luogo pubblico non vale a escluderne l'ambito applicativo, bensì irrobustisce le ragioni dei due appellanti nei termini in cui costituisce “*una considerevole ingerenza nella vita privata dei dipendenti*”<sup>383</sup>. O meglio, anche quando il luogo di lavoro è pubblico (o aperto al pubblico, secondo la nostra terminologia giuridica nazionale) l'aspettativa di protezione del diritto alla privacy del lavoratore non svanisce solo per ciò. Se fosse diversamente, il mero fatto di trovarsi in luogo pubblico determinerebbe una declaratoria d'inammissibilità del ricorso per incompatibilità con *ratione materiae* la Convenzione ai sensi dell'art. 35, par. 3, lett. a) CEDU<sup>384</sup>.

La decisione Antović e Mirković presenta un ulteriore profilo di interesse: la Corte, pur non escludendo che gli scopi perseguiti dal datore di lavoro montenegrino fossero in sé legittimi, ha ritenuto che le dichiarate finalità protettive dell'incolumità pubblica e del patrimonio dell'ente non fossero di rilevanza tale da poter efficacemente bilanciare le misure restrittive adottate dall'università datrice di lavoro, in quanto quest'ultima avrebbe ben potuto impiegare differenti mezzi a sua disposizione, meno invasivi ma ugualmente idonei ad assicurare il perseguimento di detti scopi. Non è valso a bilanciare tale giudizio di sproporzione il rilievo che l'attività di

---

<sup>382</sup> Le corti nazionali ritenevano che, essendo le aule dell'università un luogo pubblico, fosse impossibile che la videosorveglianza comportasse una violazione della vita privata dei lavoratori. Nella sentenza della Corte EDU, Antović e Mirković v. Montenegro cit. si legge al par. 14 “*(..) the monitoring of the actions of an individual in a public place (..) did not give rise to an interference with that individual's private life, which could arise once any footage of such material became publicly available*”.

<sup>383</sup> Nella sentenza Antović e Mirković v. Montenegro, 28 novembre 2017, sez. II, n. 70838/13, si legge “*developing mutual relations and constructing their social identity*”.

<sup>384</sup> Art. 35, par. 3, lett. a) CEDU: “*La Corte dichiara irricevibile ogni ricorso individuale presentato ai sensi dell'articolo 34 se ritiene che: (a) il ricorso è incompatibile con le disposizioni della Convenzione o dei suoi Protocolli, manifestamente infondato o abusivo*”.

videosorveglianza, a differenza di quanto avvenuto in López Ribalda, fosse stata effettuata in modo palese a seguito di una compiuta informazione dei lavoratori<sup>385</sup>.

## 2.2 López Ribalda e altri v. Spagna: la versione della Camera semplice

Concentrandoci ora sulla sentenza López Ribalda e altri v. Spagna, i fatti di causa risalgono al 2009 quando i ricorrenti erano dipendenti in un supermercato spagnolo con mansioni di cassiere e di assistente alle vendite. Il datore di lavoro, gestore di un supermercato spagnolo della catena M.S.A., registrate per svariati mesi una serie di discrepanze tra i livelli delle scorte di magazzino e gli incassi di fine giornata<sup>386</sup> e sospettando che ciò dipendesse dalla condotta illecita dei dipendenti, procedeva all'installazione di sistemi di videosorveglianza. La peculiarità della situazione derivava dal fatto che i sistemi di videosorveglianza impiegati erano di due tipologie: alcune telecamere, installate previa notificazione all'autorità garante spagnola e previa informativa ai lavoratori, erano collocate in posizione ben visibile, a sorveglianza dei varchi di entrata/uscita; altre invece, erano state disposte in modo che fossero nascoste ai dipendenti del supermercato, ignari dunque di tale monitoraggio, in posizione utile alla sorveglianza generalizzata e indistinta di tutto il personale di volta in volta addetto al bancone di cassa (*covert video surveillance*). Ciò avveniva nonostante il codice per la protezione dei dati personali spagnolo imponesse, senza apparenti deroghe, l'obbligo di farne comunicazione ai lavoratori in modo chiaro ed esauriente, nonché l'obbligo di compiuta informazione circa le modalità di trattamento dei dati personali acquisiti con tale mezzo. Grazie ai filmati, venivano individuati e licenziati i responsabili delle accertate sottrazioni: le telecamere avevano infatti ripreso alcuni dipendenti, intenti non solo a perpetrare furti individuali, ma anche a collaborare tra di loro e/o con alcuni clienti alla sottrazione di vari prodotti.

I lavoratori in questione separatamente, promuovevano causa dinanzi al tribunale del lavoro, lamentando una violazione dell'Estatuto de los trabajadores, nonché del diritto alla privacy tutelato dalla Costituzione spagnola<sup>387</sup>. In particolare adivano le corti nazionali contestando l'uso della videosorveglianza occulta, sulla base del fatto che quest'ultima avrebbe consentito al datore di lavoro un'indebita e arbitraria invasione della loro privacy, lamentando dunque la lesione del

---

<sup>385</sup> LOMARDI A., *Il potere di controllo del datore di lavoro alla luce della giurisprudenza CEDU*, Ricerca del Dipartimento di Diritto Pubblico dell'Università di Perugia, 18 novembre 2017.

<sup>386</sup> Nella sentenza della Corte EDU, López Ribalda e altri v. Spagna, 9 gennaio 2018, Sez. III, ricorsi nn. 1874/13 e 8567/13, si legge “*the shop supervisor identified losses in excess of EUR 7,780 in February, EUR 17,971 in March, EUR 13,936 in April, EUR 18,009 in May and EUR 24,614 in June 2009*”.

<sup>387</sup> La Costituzione spagnola del 1978 sancisce il diritto alla privacy della persona all'art. 18 come un diritto fondamentale in generale, ma ugualmente suscettibile di essere considerato un diritto del lavoro fondamentale di natura non specifica. E con la stessa natura di un diritto fondamentale, nell'art. 18 comma 4 proclama il cosiddetto “diritto al controllo dei dati” quando afferma che la legge limiterà l'uso della tecnologia dell'informazione per garantire l'onore e la privacy personale e familiare dei cittadini e il pieno esercizio dei loro diritti. Sul punto, PALOMEQUE LÒPEZ M.-ÁLVAREZ DE LA ROSA M., *Derecho del Trabajo*, Madrid, 2019.

proprio diritto alla privacy (art. 8 CEDU) e denunciando, sotto il profilo processuale, la violazione del diritto di difesa, cagionato dall'uso in giudizio dei dati occultamente carpiti quali prova a loro carico (art. 6 CEDU).

Le corti nazionali rigettavano ogni domanda ritenendo che la condotta datoriale denunciata, considerate le circostanze del caso, fosse da reputarsi lecita e proporzionata all'entità dei fatti posti a giustificazione dei licenziamenti. I tribunali spagnoli hanno dichiarato infatti tali licenziamenti appropriati, legittimi. In particolare, il giudice di prime cure riteneva il controllo realizzato nel pieno rispetto della dignità umana dei lavoratori, e dunque conforme all'art. 20 dell'Estatuto de los trabajadores<sup>388</sup>, che consente al datore di lavoro di adottare misure di monitoraggio e sorveglianza per verificare, riscontrati dei sospetti concreti, un eventuale inadempimento degli obblighi lavorativi nel rispetto della dignità umana; il giudice di appello, successivamente adito, l'Alta Corte di Giustizia della Catalogna (Tribunal Superior de Justicia de Catalunya) invece, pur riconoscendo la sussistenza di presupposti giustificativi dell'irrogazione di una sanzione amministrativa nei confronti del datore di lavoro per omessa informazione dei lavoratori in ordine all'installazione delle telecamere, sosteneva che, nel caso di specie, la videosorveglianza, ancorché occulta, fosse legittima in prima battuta perché giustificata, nella specie, dai ragionevoli sospetti di furti, in seconda battuta perché necessaria per l'adeguata protezione agli interessi patrimoniali dell'azienda, e in terzo luogo perché proporzionata, implicando il minor sacrificio possibile dei diritti dei dipendenti. Quindi il solo fatto della mancata informativa ai dipendenti non era di per sé rilevante da un punto di vista costituzionale per arrivare a dichiarare i licenziamenti intimati non giustificati. Si deve considerare ammissibile e legittima un'interferenza del datore nella sfera di riservatezza dei lavoratori purché giustificata, come nel caso in esame, da circostanziati sospetti, proporzionata, necessaria e volta a raggiungere un obiettivo legittimo.

I successivi ricorsi in Cassazione venivano dichiarati irricevibili e quelli presentati alla Corte costituzionale, per violazione degli artt. 18 e 24 della Costituzione, erano giudicati inammissibili; pertanto, esauriti i gradi di giudizio in Spagna, i dipendenti ricorrevano presso Corte europea dei diritti dell'uomo per violazione degli artt. 8 e 6 CEDU.

L'approccio seguito dai giudici spagnoli ricorda, per certi versi, il percorso giurisprudenziale che in Italia ha condotto all'elaborazione della teoria dei c.d. controlli difensivi. Tale categoria comprende, come ampiamente ricordato, quelle attività di sorveglianza a distanza, quali ad esempio il monitoraggio degli accessi alla rete internet o del sistema di posta elettronica aziendale, poste in

---

<sup>388</sup> Art. 20.3 Estatuto de los Trabajadores: “*El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad*”.

essere per mezzo di strumenti tecnologici non allo scopo di verificare l'esatto adempimento delle obbligazioni contrattuali da parte dei lavoratori, in quanto tale tradizionalmente vietato dalla formulazione letterale dell'art. 4 St. lav., bensì al fine di accertare la commissione di condotte illecite lesive del patrimonio aziendale ovvero pericolose per la sicurezza del luogo di lavoro. Si tratta di fattispecie in cui la giurisprudenza ha elaborato, sostanzialmente *praeter legem*, un'area immune dai vincoli di legittimità imposti dall'art. 4 St. lav. Analogamente, nel caso López Ribalda i giudici nazionali giudicavano la condotta datoriale legittima nonostante la legge spagnola non prevedesse alcun esplicito esonero dall'adempimento dell'obbligo di offrire ai lavoratori sottoposti a controllo una compiuta informazione preventiva<sup>389</sup>.

I lavoratori ricorrevano contro lo Stato spagnolo davanti alla Corte di Strasburgo, ai sensi dell'art. 34 CEDU, lamentando, in particolare, la violazione degli artt. 6 e 8 CEDU<sup>390</sup>. Sotto il primo profilo, sostenendo la violazione del diritto a un equo processo, i ricorrenti mettevano in evidenza che le sentenze dei giudici interni avevano fondato la legittimità del licenziamento sulle immagini registrate dalle videocamere nascoste e, pertanto, su prove ottenute illegalmente. Sotto il secondo profilo, denunciavano e, la lesione del loro diritto alla riservatezza, previsto e tutelato dall'art. 8 CEDU, lesione conseguenza della videosorveglianza predisposta dal loro datore di lavoro senza che questi li avesse preliminarmente informati, (informazione dovuta per effetto del Personal Data Protection Act), concretandosi così la cd. videosorveglianza occulta e, il fatto che la sorveglianza non fosse stata limitata nel tempo, avendo quindi ripreso l'intero staff durante tutte le ore di lavoro; infine sostenevano come l'art. 8 CEDU non dovesse essere letto solo nel senso di tutelare l'individuo dalle interferenze delle autorità pubbliche ma anche di tutelarlo nella vita privata anche nei suoi rapporti interpersonali.

---

<sup>389</sup> PERRONE F., *Corte Europea dei Diritti dell'Uomo, sentenza López Ribalda c. Spagna: la tutela della privacy sul luogo di lavoro dopo Bărbulescu 2*, su <https://www.rivistalabor.it>.

<sup>390</sup> Art. 6 CEDU:

1. *Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un tribunale indipendente e imparziale, costituito per legge, il quale sia chiamato a pronunciarsi sulle controversie sui suoi diritti e doveri di carattere civile o sulla fondatezza di ogni accusa penale formulata nei suoi confronti. La sentenza deve essere resa pubblicamente, ma l'accesso alla sala d'udienza può essere vietato alla stampa e al pubblico durante tutto o parte del processo nell'interesse della morale, dell'ordine pubblico o della sicurezza nazionale in una società democratica, quando lo esigono gli interessi dei minori o la protezione della vita privata delle parti in causa, o, nella misura giudicata strettamente necessaria dal tribunale, quando in circostanze speciali la pubblicità possa portare pregiudizio agli interessi della giustizia.*

Art. 8 CEDU:

1. *Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.*  
2. *Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui.*

La sentenza della Camera semplice della Corte EDU, resa a maggioranza il 9 gennaio 2018<sup>391</sup>, escludeva la violazione dell'art. 6 CEDU, giacché l'uso delle videoregistrazioni segretamente effettuate non era in conflitto con i requisiti di equità garantiti dall'art. 6 della Convenzione, per due ragioni: da un lato, i lavoratori licenziati avevano avuto l'ampia possibilità di contestare sia l'autenticità, che l'impiego del materiale probatorio dinanzi alle giurisdizioni nazionali, dall'altro, le registrazioni contestate non erano state l'unica prova in concreto utilizzata, essendo state valutate anche le testimonianze di altri colleghi coinvolti nei furti, del direttore del negozio e dei membri delle rappresentanze sindacali e aziendali.

Era accolta, invece, la seconda delle prospettate censure, aderendo a una nozione ampia di "vita privata" ai sensi dell'art. 8 della Convenzione.

La Corte, in particolare, osservava come "*il concetto di vita privata si estende agli aspetti relativi all'identità personale, come il nome o l'immagine di una persona (...) può includere attività di natura professionale o imprenditoriale (...) anche effettuate al di fuori della casa di una persona o di locali privati*". Da tale assunto derivava, per i giudici di Strasburgo, che la videosorveglianza nascosta di un dipendente nel suo luogo di lavoro è una considerevole intrusione nella sua vita privata. Essa comporta una documentazione riproducibile della condotta di una persona sul suo posto di lavoro, e il dipendente non può eluderla, essendo obbligato a svolgere il lavoro in quel determinato luogo<sup>392</sup>. Ciò vale a sgomberare il campo dall'idea, spesso sottesa alle impostazioni difensive dei datori di lavoro costituiti in giudizio, che il lavoratore, per il solo fatto di trovarsi all'interno dei locali aziendali o impegnato nell'utilizzazione di beni strumentali aziendali (come l'e-mail o un laptop aziendale), non possa avanzare alcuna pretesa di protezione del proprio diritto alla vita privata. Così argomentando, la Corte disattendeva le difese del governo spagnolo che, quanto alla violazione dell'art. 8, forte del fatto che le misure erano state predisposte da una società privata, sosteneva la sua immunità da qualunque addebito di responsabilità: il governo spagnolo non negava che l'installazione dei sistemi di videosorveglianza occulta senza previa informativa ai lavoratori fosse in contrasto con gli artt. 18 comma 4 e 8, rispettivamente della Costituzione spagnola e della CEDU, ma assumeva di non esserne responsabile in quanto all'installazione aveva provveduto una compagnia privata. Tuttavia, per i giudici di Strasburgo l'art. 8 CEDU doveva essere interpretato non solo come norma di protezione dell'individuo da interferenze arbitrarie da

---

<sup>391</sup> Corte EDU, López Ribalda e altri v. Spagna, 9 gennaio 2018, sez. III, ricorsi nn. 1874/13 e 8567/13, su <https://hudoc.echr.coe.int/>.

<sup>392</sup> Ibidem "*the covert video surveillance of an employee at his or her workplace must be considered, as such, as a considerable intrusion into his or her private life. It entails a recorded and reproducible documentation of a person's conduct at his or her workplace, which he or she, being obliged under the employment contract to perform the work in that place, cannot evade*".

parte delle autorità pubbliche, ma anche come disposizione impositiva di obblighi di intervento a carico dello Stato, tenuto pertanto ad adottare le misure atte ad assicurare il rispetto della privacy anche nei rapporti interprivati. Proprio queste misure, secondo quanto emerge dalla decisione della Corte, erano state, nel caso di specie, disattese dal governo spagnolo dimostratosi incapace di garantire il “giusto equilibrio” tra il diritto dei lavoratori al rispetto della riservatezza e quello del datore alla tutela degli interessi aziendali nonché, in senso lato, della sua proprietà, non avendo il datore di lavoro rispettato l'obbligo, sancito dalla sezione 5 della legge spagnola sulla protezione dei dati personali, di informare gli interessati della predisposizione e dell'attivazione di un mezzo di raccolta e trattamento dei loro dati personali.

L'art. 8 della CEDU, presenta una struttura bipartita: esso è costituito da un primo paragrafo enunciante il contenuto del diritto tutelato (“*ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza*”), e da un secondo paragrafo che enuclea i tre presupposti in presenza dei quali ogni Stato membro è legittimato a sottoporre a restrizioni (interferences) l'esercizio del diritto definito dal primo paragrafo: la restrizione deve trovare fondamento nella legge (*in accordance with the law*); la restrizione deve essere giustificata dalla necessità di perseguire almeno una delle finalità legittime tassativamente elencate dalla norma (*a legitimate aim*); la restrizione deve essere necessaria in una società democratica (*necessary in a democratic society*). L'art. 8 dunque impone allo Stato l'obbligazione positiva di adottare le misure legislative necessarie a munire di una valida base legale le restrizioni del diritto alla privacy che lo Stato ritiene di autorizzare.

La *ratio decidendi* della sentenza ha il suo perno nell'ultimo dei tre presupposti contemplati dall'art. 8, par. 2, CEDU, il cui nucleo sostanziale è rappresentato dal principio di proporzionalità che deve intercorrere tra una determinata restrizione del diritto autorizzata dallo Stato e il fine (legittimo) concretamente perseguito. La Corte EDU ha rilevato, come anticipato, che, nel caso di specie, l'attività di sorveglianza occulta si è risolta in una misura di controllo diretta a colpire indistintamente l'intero staff impiegato presso il punto vendita, e, in quanto tale, appare sproporzionata rispetto al fine (in sé lecito) di tutelare l'interesse organizzativo-patrimoniale del datore di lavoro. Ha pertanto ritenuto che lo Stato convenuto, omettendo di sanzionare tale sproporzionalità, abbia fallito il giudizio di bilanciamento imposto dall'art. 8, par. 2, CEDU. Ad avviso della Corte, infine, la durata prolungata della videosorveglianza e le sue potenzialità di controllo generalizzato e indiscriminato di tutti i dipendenti escludevano la proporzionalità della misura, atteso che gli interessi datoriali, ripetiamo di per sé legittimi, avrebbero potuto essere tutelati,

almeno in parte, con mezzi differenti, per esempio, informando anticipatamente, anche se genericamente, i lavoratori.

A tal proposito, nella sentenza del 9 gennaio 2018, viene effettuato un parallelo con il caso Köpke v. Germania, il quale presenta tante assonanze, quanto importanti divergenze con il caso López Ribalda. Anche in Köpke v. Germania, a fronte di una serie di ammanchi verificatisi all'interno del deposito bevande di un supermercato, il datore di lavoro aveva deciso di porre sotto videosorveglianza, all'insaputa dei dipendenti, il locale adibito a deposito bevande e la postazione di cassa. In tal caso la Corte ricorda, e non nega, di aver accettato una registrazione effettuata con una telecamera nascosta. Tuttavia nel caso tedesco i sospetti e le conseguenti attività di controllo si concentravano su due particolari lavoratori, anziché indirizzarsi indistintamente verso la generalità dell'organico aziendale ed erano limitate nel tempo, essendo durate due settimane, a differenza della misura adottata dal datore di lavoro spagnolo che, basata su un generale sospetto comportante una videosorveglianza di tutto il personale, era temporalmente illimitata. Tali significative differenze rispetto alla vicenda López Ribalda erano state valorizzate dalla Corte al fine di giustificarne la predisposizione perché circoscritte e quindi poco invasive della riservatezza dei lavoratori, ritenendosi che lo scopo legittimo di tutela degli interessi organizzativo-patrimoniali dell'azienda fosse stato in concreto perseguito assicurando il giusto equilibrio tra il diritto del richiedente alla tutela della sua vita privata e quello del datore alla protezione dell'impresa<sup>393</sup>. La Corte, in particolare, ha ritenuto compiuto dalle corti tedesche un corretto bilanciamento degli interessi in gioco, riconoscendo che lo scopo legittimo di tutela del patrimonio aziendale fosse stato in concreto perseguito, diversamente da quanto avvenuto in López Ribalda, facendo uso di misure restrittive risultanti le meno invasive tra quelle disponibili.

Se ne deduce che, nella prospettiva convenzionale, assume una notevolissima rilevanza discrezionale la circostanza che l'atto di controllo sia circoscritto a un novero di destinatari determinati, piuttosto che indiscriminatamente esteso a un gruppo di lavoratori. La Corte EDU non può condividere pertanto nel caso spagnolo il punto di vista delle corti domestiche sulla proporzionalità delle misure adottate dal gestore del supermercato con lo scopo legittimo di proteggere gli interessi del datore di lavoro a fronte del fatto che la videosorveglianza è stata predisposta senza limiti temporali e senza informativa, che può anche essere, ricordiamo, generale, ai lavoratori.

---

<sup>393</sup> BUFFA F.- PERRONE F., *La rilevanza dell'informazione preventiva nei controlli a distanza sul luogo di lavoro*, su <https://www.questionegiustizia.it>.

### **Segue. Una lettura congiunta delle sentenze della Corte EDU**

A questo punto, prima di affrontare la sentenza López Ribalda e altri v. Spagna del 17 ottobre 2019 con cui la Corte EDU ha fatto marcia indietro rispetto a quanto statuito nel gennaio 2018, è opportuno analizzare gli aspetti comuni ai tre casi, come evidenziati sopra, che rendono possibile un'unica lettura delle decisioni della Corte EDU.

Esse seguono uno schema simile: punto di partenza è sempre la determinazione della definizione di “vita privata” ai sensi dell’art. 8 della Convenzione, dei suoi confini e limiti. Nei casi Bărbulescu e López Ribalda, inoltre, la Corte è stata chiamata a svolgere un’altra riflessione preliminare: trattandosi di una controversia in materia di lavoro tra soggetti privati, i giudici si sono chiesti quali fossero i limiti dell’intervento dello Stato nella garanzia del diritto alla riservatezza in tale particolare contesto. La Corte passa poi a esaminare il bilanciamento, effettuato dai giudici nazionali, tra tutela della privacy del lavoratore e diritto del datore a effettuare controlli che possano garantire una efficace ed efficiente gestione delle attività aziendali: da questa analisi deriva la decisione finale sulla sussistenza della violazione dell’art. 8 CEDU e quindi della compressione illegittima della riservatezza dei dipendenti. Quanto al primo aspetto, in questa serie di pronunce, la Corte EDU chiarisce con precisione cosa possa rientrare nell’ambito di applicazione dell’art. 8 della Convenzione. Questa disposizione è volta a proteggere il diritto allo sviluppo della persona nella sua dimensione privata, da intendersi non solo come *inner circle* all’interno del quale i singoli soggetti vivono la loro vita personale e dal quale decidono di escludere il mondo esterno<sup>394</sup>, ma come comprensiva anche della *private social life*, considerata come una delle dimensioni nelle quali si esplica e si sviluppa la personalità dell’individuo<sup>395</sup>. Il concetto di “vita privata” dunque è da interpretarsi estensivamente, come comprensivo anche della vita che l’individuo svolge nell’ambiente lavorativo o con riferimento alle attività che hanno luogo in un contesto pubblico. Ne deriva ad esempio che nel caso Antovič, il semplice fatto che, come detto, i professori universitari svolgano il proprio lavoro in un luogo pubblico, non comporta la “fuoriuscita” di queste attività dalla “vita privata” dei ricorrenti, anzi, le aule universitarie sono l’ambiente in cui questi soggetti interagiscono con gli studenti. Prendendo in considerazione poi le operazioni di videosorveglianza, i giudici hanno affermato in maniera decisa come la registrazione delle attività lavorative (nel caso López Ribalda, avvenuta all’insaputa dei dipendenti), debba di per sé essere considerata una forte

---

<sup>394</sup> Corte EDU, Antovič e Mirkovič v. Montenegro, 28 novembre 2017, Sez. II, ricorso n. 70838/13, par. 41, su <https://hudoc.echr.coe.int/>.

<sup>395</sup> Corte EDU, Bărbulescu v. Romania, 5 settembre 2017, Grande Camera, ricorso n. 61496/08, par. 70-71, su <https://hudoc.echr.coe.int/>.

ingerenza nella vita privata dell'individuo<sup>396</sup>. Affermata l'applicabilità dell'art. 8 della Convenzione, la Corte EDU si chiede cosa implichi, nei confronti degli Stati, la garanzia stabilita in quella disposizione: in altre parole, trattandosi nelle controversie *Bărbulescu* e *López Ribalda* di un rapporto tra soggetti privati, come si sostanzia il dovere degli Stati di rispettare la Convenzione e di assicurare a tutti i diritti e le libertà in essa affermati (art. 1 Convenzione EDU). Ebbene secondo i giudici di Strasburgo, l'art. 8, per quanto rivolto a proteggere gli individui contro le interferenze arbitrarie delle pubbliche autorità, non stabilisce solamente obbligazione negativa, ovvero sia un'astensione dello Stato da queste interferenze, ma impone anche un'obbligazione positiva, che deve concretarsi in un effettivo rispetto della vita privata. Tale obbligazione si traduce nei fatti nella predisposizione di leggi a tutela della privacy, così come nell'intervento di garanzia degli organi di giustizia. In questo contesto, il fatto che il rapporto entro al quale il diritto si sostanzia sia sussistente tra soggetti privati e pubblici o solo privati, non comporta nessuna differenziazione rispetto alle obbligazioni in capo allo Stato. Nell'adempimento di queste obbligazioni, agli Stati è ovviamente riconosciuto un ampio ma non illimitato margine di discrezionalità per stabilire quali misure adottare<sup>397</sup>. Ne consegue che il potere di monitoraggio e controllo attribuito al datore deve sempre essere controbilanciato da adeguate garanzie di tutela della riservatezza, che impediscano l'insorgere di abusi. Proprio in questo quadro, si inserisce il vaglio della Corte EDU, che è dunque stata chiamata a pronunciarsi sulla correttezza ed equità del bilanciamento operato dal legislatore o giudice nazionale tra diritti e interessi contrapposti. I giudici di Strasburgo quindi non affermano l'illegittimità *tout court* dei controlli nei confronti dei lavoratori: ciò che la Grande Camera stabilisce nella sentenza *Bărbulescu*, confermata anche nelle successive pronunce, è una sorta di *vademecum*, valido per le autorità nazionali ma anche, prima ancora e indirettamente, per il datore di lavoro stesso, nel quale fissa una serie di criteri e di questioni che non possono non essere considerati nelle operazioni di bilanciamento. In altre parole vengono delineati, in termini astratti e generali, il ragionamento logico e i quesiti che i giudici devono porsi per determinare la legittimità della misura di controllo attuata dal datore. È essenziale dunque valutare, come anticipato: a) se il dipendente sia stato preventivamente informato del possibile svolgimento di controlli; b) se il datore abbia dato chiare informazioni sull'entità, sul livello di ingerenza e intrusione, sulla durata e sull'estensione del controllo (se ad esempio si estenda anche al contenuto della corrispondenza),

---

<sup>396</sup> Cfr. Corte EDU, *López Ribalda e altri v. Spagna*, 9 gennaio 2018, sez. III, ricorsi nn. 1874/13 e 8567/13, par. 59, su <https://hudoc.echr.coe.int/>; Corte EDU, *Köpke v. Germania*, 5 ottobre 2010, ricorso n. 420/07, su <https://hudoc.echr.coe.int/>.

<sup>397</sup> Se ad esempio intervenire con una specifica disposizione normativa che regoli il controllo dalla corrispondenza telematica da parte del datore. Nella sentenza *Bărbulescu v. Romania* decisa dalla Grande Camera al par. 120 si legge: "*nevertheless, the discretion enjoyed by States in this field cannot be unlimited*".

nonché sul numero di soggetti che possono avere accesso agli esiti dei controlli; c) se le ragioni addotte dal datore per motivare le attività di controllo siano legittime; d) se non vi siano altre misure a disposizione del datore di lavoro, meno invasive di quelle adottate; e) quali siano le conseguenze del monitoraggio; f) se siano previste misure di salvaguardia adeguate per il dipendente<sup>398</sup>. A ciò deve aggiungersi, inoltre, la garanzia, a favore del lavoratore, di poter esperire rimedi di fronte ad un giudice nazionale, il quale sarà chiamato a determinare se e come i criteri sopra delineati siano stati effettivamente osservati: viene quindi ribadita la portata di quell'obbligazione positiva in capo agli Stati, che sono chiamati a tutelare il rispetto dell'art. 8 della Convenzione anche mediante la garanzia di un vaglio giurisprudenziale effettivo. La Grande Camera, dopo aver fissato in una sintesi chiara e puntuale i criteri generali in materia, li traspone poi nel caso concreto in esame, evidenziando le mancanze delle corti rumene e della stessa Corte EDU, sez. IV: quest'ultima infatti, pur dovendosi attenere alla ricostruzione dei fatti svolta dai giudici nazionali, non aveva comunque valutato se i quesiti sopra indicati fossero stati debitamente considerati nei precedenti gradi di giudizio. In particolare, ciò che era stato comprovato e considerato era semplicemente la conoscenza da parte dell'ingegnere rumeno, della sussistenza di una politica interna, dai confini piuttosto ampi e vaghi, sui limiti dell'utilizzo di internet e di altri strumenti telematici di proprietà dell'azienda: non era stata invece verificata e provata l'esistenza di una specifica preventiva informazione in merito all'inizio, alla durata, alla natura, all'estensione di controlli della corrispondenza da parte del datore. Non era stato effettuato neppure un scrutinio sulla legittimità dello scopo e sulla necessità della decisione del datore di dare avvio al monitoraggio: nonostante fosse stata citata l'esigenza di verificare il rispetto delle regole aziendali da parte dei lavoratori, al fine di prevenire o accertare il danneggiamento di sistemi informatici, l'esistenza di attività informatiche illegali o la violazione dei segreti industriali, non era stata mostrata dal datore alcuna prova di legittimi sospetti o di danni subiti, tale da giustificare un intervento di controllo. Neppure le conseguenze del monitoraggio o la sussistenza di mezzi alternativi di sorveglianza, meno invasivi per la riservatezza del lavoratore, erano stati considerati dai giudici quali elementi determinanti per stabilire l'equità del bilanciamento tra contrapposti interessi. Dall'esame di tutti questi criteri, la Grande Camera, ribaltando la decisione della quarta sezione, aveva rilevato il fallimento delle corti nazionali del proprio compito di proteggere il diritto alla vita privata del lavoratore e conclude affermando la sussistenza della lesione dell'art. 8 della Convenzione.

---

<sup>398</sup> Corte EDU, *Bărbulescu v. Romania*, 5 settembre 2017, Grande Camera, ricorso n. 61496/08, par. 121, su <https://hudoc.echr.coe.int/>.

Alla stessa conclusione la Corte EDU perviene, sia nel caso Antovič, che nel più recente caso López Ribalda, in materia di videosorveglianza<sup>399</sup>: partendo dalle stesse premesse del caso Bărbulescu, la Corte EDU procede valutando, in entrambi i casi, in primis la sussistenza di una normativa nazionale in materia di controlli dei datori sui luoghi di lavoro, per poi vagliare nello specifico le misure di monitoraggio adottate, alla luce di quei criteri di legittimità dello scopo perseguito, proporzionalità e necessità, delineati dalla Grande Camera nel precedente richiamato. Nel caso Antovič la Corte, valutando questi elementi, giunge alla conclusione, espressa in termini estremamente sintetici, che le misure adottate dal preside di facoltà non fossero conformi alle disposizioni previste dal personal data protection act montenegrino<sup>400</sup>: ne deriva che l'ingerenza nel diritto alla riservatezza dei professori ricorrenti, posta in essere dal datore di lavoro, già solo sulla base di questo elemento, sia da considerarsi in violazione dell'art. 8 della Convenzione. Nel caso López Ribalda, invece, la Corte EDU ha svolto un'indagine più approfondita rispetto alla sola valutazione della sussistenza di una specifica normativa interna: nel caso dei cassieri spagnoli infatti i giudici di Strasburgo hanno rilevato il mancato rispetto da parte del datore dell'obbligo di una previa informativa del lavoratore della predisposizione di forme di sorveglianza a distanza, così come previsto dalle norme nazionali in materia di tutela dei dati. Ma non si sono limitati a questo: la Corte ha vagliato le misure adottate dal datore sulla base dei criteri-guida di necessità, legittimità e proporzionalità, delineati nel caso Bărbulescu<sup>401</sup>. Ebbene, nel caso López Ribalda la Corte giunge a una soluzione completamente opposta rispetto a quella delle corti nazionali: elementi determinanti di questo esito, come visto, sono stati la mancata limitazione temporale delle operazioni di videosorveglianza, protrattesi per un periodo prolungato di tempo, così come l'assenza di un target ben specifico<sup>402</sup>. Dall'analisi di tutti questi aspetti fattuali, la Corte EDU giunge alla conclusione

---

<sup>399</sup> Cfr. CALIFANO L. - FIORILLO V., *Videosorveglianza*, in BIFULCO R. - CELOTTO A. - OLIVETTI M. (a cura di), *Digesto delle discipline pubblicistiche*, Torino, 2015, pp. 503 ss.; PAMPALONE E., *La videosorveglianza in Europa: un fragile equilibrio tra "controllo" e "libertà"*, in TORRE A. (a cura di), *Costituzioni e sicurezza dello Stato*, Santarcangelo di Romagna, 2013; nel contesto normativo italiano: BELLAVISTA A., *Gli accordi sindacali in materia di controlli a distanza sui lavoratori*, in *Il lavoro nella giurisprudenza*, 8-9/2014, pp. 737 ss.; GRANDI M., *Impianti di videosorveglianza in ambienti di lavoro*, Padova, 2017.

<sup>400</sup> La normativa in esame infatti permetteva la predisposizione di videosorveglianza solo in aree di accesso ai locali lavorativi o, eccezionalmente, in altre zone nelle quali vi fosse lo scopo di proteggere la sicurezza di persone, beni o dati confidenziali, laddove questa tutela non potesse essere ottenuta in altro modo (sezione 35 e 36 del Personal Data Protection Act). Nel caso dell'Università montenegrina non solo le telecamere erano posizionate nelle aule, ma non era neppure stata provata la sussistenza di minacce a beni o persone. Le corti nazionali tuttavia non erano giunte a considerare la questione della coerenza dei controlli rispetto alla normativa interna poiché partivano dal presupposto che la videosorveglianza non costituisse una ingerenza nella vita privata dei professori (sent. Antovič e Mirkovič v. Montenegro, par. 56; 58-59).

<sup>401</sup> FORMICI G., op. cit.

<sup>402</sup> Viene in questo caso richiamata la già citata decisione Köpke v. Germania, nella quale invece la Corte EDU era arrivata a un esito opposto: in quel caso infatti non sussisteva una normativa interna specifica in materia di controllo svolto dal datore di lavoro, la sorveglianza effettuata era mirata a soli due dipendenti sospettati, limitata nel tempo (sole due settimane) e ai dati registrati avevano avuto accesso solo un numero limitato di persone. In tale specifico contesto

che la misura di controllo adottata dal datore non possa essere considerata proporzionata e che quindi non sia stato effettuato un equo bilanciamento dei diritti in gioco. Riassuntivamente, può essere affermato che la videosorveglianza non comporti di per sé una interferenza nella vita privata, ma ciò dipende da quelle particolari circostanze ed elementi, delineati poi chiaramente dalla Grande Camera e che le autorità sono chiamate a considerare nel caso specifico.<sup>403</sup>

### **2.3 López Ribalda e altri v. Spagna: il cambio di rotta della Grande Camera**

Con la sentenza López Ribalda e altri v. Spagna del 17 ottobre 2019, la Corte EDU ha riaperto il dibattito relativo all'estensione della tutela del diritto alla privacy sul posto di lavoro e nella specie, in riforma del precedente della Camera semplice, sposa un'interpretazione dell'art. 8 della Convenzione che, alla luce delle peculiarità del caso concreto, porta la Corte a negarne, sostanzialmente, la violazione. La Grande Camera della Corte di Strasburgo ha così stabilito che è ammissibile, non configurandosi violazione dell'articolo 8 CEDU, l'installazione di telecamere nascoste sul luogo di lavoro nei casi in cui vi siano fondati e ragionevoli sospetti di furti commessi dai lavoratori ai danni del patrimonio aziendale, l'area oggetto di ripresa (aperta al pubblico) risulti circoscritta, per un limitato periodo di tempo, che le immagini siano utilizzate quali mezzi di prova e che non risulti possibile ricorrere ad altri mezzi meno invasivi.

Le ricorrenti in tale sede hanno opposto che a costituire violazione della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali è stato il rifiuto, da parte dei tribunali nazionali, di trarre le appropriate conseguenze dall'omesso adempimento da parte del datore di lavoro dell'obbligazione legale, su di lui gravante, di fornire informazione preventiva ai lavoratori. La Corte sottolinea che le autorità nazionali devono garantire che l'introduzione da parte di un datore di lavoro di misure di controllo che incidono sul diritto al rispetto della vita privata dei suoi dipendenti sia *“proporzionata ed accompagnata da adeguate e sufficienti garanzie contro gli abusi”*, avendo le stesse autorità non solo obblighi negativi di astensione ma anche, e *a fortiori*, positivi doveri di intervento. Quanto al vaglio di legittimità-proporzionalità della misura, la Corte

---

dunque i giudici di Strasburgo ritenevano la videosorveglianza proporzionata, concludendo per l'inammissibilità del ricorso.

<sup>403</sup> Di minor rilievo, rispetto all'argomento principale di questo elaborato, è la posizione della Corte rispetto alla violazione dell'art. 6 della Convenzione. Si vuole solo ricordare che, sotto questo profilo, i giudici di Strasburgo concludono ritenendo che i video, ottenuti violando il diritto alla riservatezza, possano comunque essere utilizzati come prove nell'ambito di un procedimento giudiziario. Ribadendo l'impossibilità per la Corte EDU di vagliare l'ammissibilità delle prove, essa è comunque chiamata a decidere se il processo nel suo complesso sia stato equo: nel caso in esame, i giudici ritengono innanzitutto come i ricorrenti avessero avuto modo, nelle preposte sedi, di contestare la validità e autenticità delle registrazioni e come, soprattutto, gli esiti della videosorveglianza non costituissero in ogni caso le uniche prove addotte contro i ricorrenti. Il fatto che i filmati fossero stati raccolti in contrasto con l'art. 8, non giunge quindi a determinare automaticamente una violazione del diritto al giusto processo, tutelato dall'art. 6 della Convenzione.

richiama la decisione del caso *Bărbulescu v. Romania*, ritenendo che i principi ivi sanciti<sup>404</sup>, e già ampiamente ricordati, siano applicabili, con gli opportuni adattamenti, anche quando il controllo datoriale sia realizzato, come nel caso di specie, non già con l'accesso alla corrispondenza del lavoratore, ma attraverso la predisposizione di sistemi di videosorveglianza. Sulla base di tali coordinate la Corte, pur concordando con la pronuncia resa dalla Camera semplice quanto alla esclusione della violazione dell'art. 6 CEDU, ribadita all'unanimità, esclude, sia pure con tre voti contrari, la violazione dell'art. 8 CEDU.

La Grande Camera giunge a tale conclusione facendo leva su considerazioni che valorizzano al massimo le peculiarità del caso concreto.

La Corte innanzitutto rileva che i tribunali del lavoro hanno identificato i vari interessi in gioco, facendo espresso riferimento sia al diritto dei ricorrenti al rispetto della loro vita privata, sia alla necessità di individuare un corretto punto di bilanciamento tra tale diritto e quello del datore di lavoro ad assicurare un'agevole gestione della società per mezzo dell'esercizio dei propri poteri organizzativi. Inoltre ricorda che le corti domestiche hanno sia ritenuto l'installazione di strumenti di videosorveglianza giustificata da ragioni legittime, e in particolare dal sospetto, sollevato dal manager del supermarket, di commissione dei furti, sia preso in considerazione l'interesse legittimo del datore di lavoro ad assumere misure dirette a scoprire e punire i responsabili di tali perdite economiche, per assicurare protezione al proprio diritto di proprietà e all'interesse al regolare funzionamento della propria società. A questo punto la Grande Camera condivide quanto statuito dalle corti domestiche che, esaminando l'estensione dell'attività di monitoraggio e il grado d'intrusione nella privacy dei ricorrenti, hanno ritenuto che la misura fosse stata limitata sia rispetto ai luoghi, sia rispetto ai dipendenti oggetto di videosorveglianza e che la durata dell'attività di sorveglianza non aveva ecceduto quanto necessario all'esigenza di riscontrare la fondatezza dei sospetti di furto. La Corte rileva, infatti, che il monitoraggio non si è esteso all'intero negozio, ma è stato specificamente diretto alle aree, limitate, dove si trovavano le casse, vale a dire il luogo in cui i furti erano stati verosimilmente commessi.

A tal punto non si può sorvolare sul fatto che la Grand Chamber aderisce, ancora una volta, a una concezione ampia di "vita privata" tale da ricomprendere molteplici aspetti dell'identità fisica e sociale della persona, ivi inclusi, in particolare, il nome, l'immagine e le attività lavorative con conseguente conferma dell'applicabilità anche a tale ultimo ambito dell'art. 8 CEDU: le prestazioni lavorative erano adempiute in un luogo aperto al pubblico, in una posizione lavorativa comportante permanente contatto con i clienti. La Corte è fautrice della necessità di distinguere, nell'analisi della

---

<sup>404</sup> Cfr. Corte EDU, *Bărbulescu v. Romania*, 5 settembre 2017, Grande Camera, ricorso n. 61496/08, par. 121-122, su <https://hudoc.echr.coe.int/>.

proporzionalità dell'attività di videosorveglianza, i vari luoghi in cui il monitoraggio è stato eseguito, alla luce del grado di protezione della privacy che un lavoratore può ragionevolmente aspettarsi. È legittimo ritenere che tale aspettativa sia molto alta in luoghi che sono per natura privati, quali bagni e guardaroba, dove è giustificato un innalzamento della soglia di protezione, o addirittura l'interdizione totale. La soglia di tutela rimane alta in luoghi chiusi come gli uffici; è evidentemente inferiore in luoghi che sono visibili o accessibili a colleghi oppure, come nel caso di specie, al bacino del pubblico. Se è vero che la registrazione è stata compiuta in modo generalizzato, in modo tale che tutti i lavoratori nell'area della cassa fossero registrati, e non solo quelli su cui il datore di lavoro aveva dei sospetti, ciò era dovuto al fatto che quella era l'area in cui si erano registrate le rapine, sottolineando poi che si tratta di un'area aperta al pubblico, in cui pertanto l'attesa della privacy è inferiore, tanto più che solo persone specifiche avevano accesso alle registrazioni<sup>405</sup>, quindi l'impatto sulla privacy non era di gravità significativa. Il giudice europeo ritiene che l'intrusione nella sfera di riservatezza dei ricorrenti non abbia raggiunto, nel caso *de quo*, un "livello elevato di serietà".

Quanto all'estensione temporale della misura di videosorveglianza, sebbene la durata prevista dalle registrazioni con telecamere nascoste non fosse stata impostata al momento del fissaggio dei sistemi, in pratica si è protratta per soli dieci giorni ed è cessata non appena sono stati individuati i responsabili del fatto. La durata dell'attività di videosorveglianza non sembra essere di per sé eccessiva, ciò vale anche in relazione al caso Köpke, in cui la durata è stata pari a 14 giorni, e che la Corte ha ritenuto non sproporzionata. Inoltre la Corte EDU tiene presente l'interesse legittimo del gestore del supermercato a installare le telecamere, ovverosia quello di prevenire i furti e identificare i responsabili di quelli già perpetrati; sebbene la Corte rilevi che sarebbe stato auspicabile che le corti domestiche spagnole avessero valutato in modo più dettagliato la possibilità che il datore di lavoro utilizzasse mezzi meno invasivi rispetto alle telecamere nascoste, insiste sul fatto che, come stabilito dai tribunali spagnoli, il datore di lavoro non solo ha cercato di prevenire i furti, ma anche di identificare i responsabili e che la notifica della presenza delle telecamere avrebbe reso impossibile quanto sopra. Dunque nessuna misura alternativa poteva essere efficacemente adottata atteso che "la fornitura di informazioni a qualsiasi membro del personale avrebbe potuto vanificare lo scopo della videosorveglianza, che era scoprire i responsabili dei furti, ma anche ottenere prove da utilizzare per i procedimenti disciplinari contro di loro". Con riferimento alla preliminare informazione dei dipendenti, pacificamente avvenuta in modo generico e parziale, la Grand Chamber chiarisce che la stessa rappresenta solo uno dei criteri, pertanto

---

<sup>405</sup> Si tratta solo il manager del supermarket, il legale rappresentante della società e il rappresentante sindacale.

sintomatici e non tassativi, da considerare per vagliare la proporzionalità delle misure di controllo adottate dal datore di lavoro e che, nel caso di specie, la violazione da parte del datore del dovere di informazione preventiva, esplicita, precisa e inequivocabile, di cui alla Sezione 5 della Legge spagnola sulla protezione dei dati personali<sup>406</sup>, non è in grado di inficiare la proporzionalità della misura essendo rispettati gli altri criteri. Così, tenuto conto del concreto grado d'invasione della riservatezza dei dipendenti e dei motivi legittimi che lo giustificano, la Grande Camera sancisce chiaramente la proporzionalità della misura e, di conseguenza, il rispetto dell'art. 8 CEDU.

Nella sentenza si legge che, *“mentre, in generale, il minimo sospetto di appropriazione indebita o qualsiasi altro illecito da parte dei dipendenti non può giustificare l'installazione di dispositivi di videosorveglianza occulta da parte del datore di lavoro, l'esistenza del ragionevole sospetto che sia stato commesso un grave reato e l'entità dei danni accertati nel caso di specie pare rappresentare un'adeguata giustificazione. Ciò è tanto più vero in una situazione in cui il buon funzionamento di un'azienda è messo in pericolo non solo dal sospetto comportamento scorretto di un singolo dipendente, ma piuttosto dal sospetto di un'azione concertata da parte di più dipendenti, poiché ciò crea un'atmosfera generale di sfiducia nel luogo di lavoro. In tali circostanze, viste le significative garanzie fornite dal quadro giuridico spagnolo, compresi i rimedi che le ricorrenti non hanno utilizzato, e l'importanza delle ragioni che giustificano la videosorveglianza, come rilevato dai tribunali nazionali, la Corte conclude che le autorità nazionali non sono venute meno ai loro*

---

<sup>406</sup> Che, sul punto, prevede:

Sezione 5 - Diritto all'informazione sulla raccolta di dati

1. Gli interessati i cui dati personali sono richiesti devono essere preventivamente, esplicitamente, precisamente e inequivocabilmente informati di quanto segue:

- a) l'esistenza di un file di dati personali o il fatto che i dati saranno trattati, lo scopo e i destinatari delle informazioni;
- (b) la natura obbligatoria o facoltativa della loro risposta alle domande poste;
- (c) le conseguenze della fornitura o del rifiuto di fornire i dati;
- (d) l'esistenza di diritti di accesso, rettifica, cancellazione e opposizione;
- (e) l'identità e l'indirizzo del responsabile del trattamento o, se del caso, del suo rappresentante.

(...)

4. Laddove i dati personali siano stati raccolti senza che l'interessato sia contattato, la persona deve essere informata in modo espresso, preciso e inequivocabile dal gestore del file o dal suo rappresentante, entro tre mesi dalla registrazione dei dati, tranne se l'interessato è già stato informato del contenuto del trattamento, dell'origine dei dati e delle informazioni di cui alle lettere (a), (d) ed (e) della sottosezione 1 della presente sezione.

5. Le disposizioni della precedente sottosezione non si applicano nei casi in cui la legge disponga espressamente diversamente, laddove il trattamento dei dati abbia scopi storici, statistici o scientifici o laddove sia impossibile informare l'interessato o qualora ciò implichi un sforzo sproporzionato secondo il parere dell'Agenzia per la protezione dei dati o dell'organismo regionale corrispondente, tenuto conto del numero di interessati, dell'età dei dati e delle possibili misure di compensazione. Inoltre, le disposizioni della precedente sottosezione non si applicano anche se i dati sono ottenuti da fonti accessibili al pubblico e sono destinati a pubblicità o ricerche di mercato, nel qual caso ogni comunicazione inviata all'interessato deve informarlo dell'origine dei dati, l'identità della persona/entità responsabile del trattamento dei dati e i diritti dell'interessato.

*obblighi positivi ai sensi dell'articolo 8 della Convenzione. Di conseguenza, non vi è stata violazione di tale disposizione*<sup>407</sup>.

La sentenza sul caso López Ribalda conferma, dunque, solo in parte l'iter logico già utilizzato in Bărbulescu: non solo la Corte rinuncia a richiedere il rispetto di tutti e sei i requisiti, ma arriva a costruirne, implicitamente, una sorta di gerarchia interna. A conferma di ciò, i giudici evidenziano come la mancanza di un avviso rivolto ai dipendenti circa l'installazione di un sistema di videosorveglianza sia solo uno dei criteri utilizzati per stabilire la proporzionalità di una misura; se questa informativa non viene garantita, anche per una mancanza del datore di lavoro, non vi è comunque violazione della norma ma, al più, si considera in maniera più stringente *“the safeguards deriving from the other criteria will be all the more important”*<sup>408</sup>.

Dunque, a fronte di quanto detto, la nuova risoluzione della CEDU sembra aprire le porte alla possibilità di accettare l'uso di telecamere nascoste senza nemmeno avvisare i lavoratori della loro presenza, ma a condizione che si ricada in determinate situazioni estreme<sup>409</sup>. A sottolineare l'importanza e necessità di evitare che la sorveglianza occulta non diventi prassi ordinaria è intervenuto Antonello Soro, l'allora presidente dell'autorità garante per la protezione dei dati personali, che sulla appena esaminata sentenza della Corte di Strasburgo ha affermato come *“da una parte giustifica, nel caso di specie, le telecamere nascoste, dall'altra conferma però il principio di proporzionalità come requisito essenziale di legittimazione dei controlli in ambito lavorativo. L'installazione di telecamere nascoste sul luogo di lavoro è stata infatti ritenuta ammissibile dalla Corte solo perché, nel caso che le era stato sottoposto, ricorrevano determinati presupposti: vi erano fondati e ragionevoli sospetti di furti commessi dai lavoratori ai danni del patrimonio aziendale, l'area oggetto di ripresa (peraltro aperta al pubblico) era alquanto circoscritta, le videocamere erano state in funzione per un periodo temporale limitato, non era possibile ricorrere a mezzi alternativi e le immagini captate erano state utilizzate soltanto a fini di prova dei furti commessi. La videosorveglianza occulta è, dunque, ammessa solo in quanto extrema ratio, a fronte*

---

<sup>407</sup> Non sono mancate, in seno allo stesso collegio, opinioni discordanti. Si tratta del parere dissenziente comune di tre giudici (Ganna Yudkivska, Yonko Grozev, Vincent A. De Gaetano) che, preoccupati dalla crescente ingerenza delle nuove tecnologie, hanno affermato che, senza ampie garanzie procedurali, neanche l'esistenza del ragionevole sospetto di una grave condotta scorretta è sufficiente a giustificare l'impiego della videosorveglianza occulta sul posto di lavoro comportando, per ciò solo, la violazione dell'art. 8 CEDU.

<sup>408</sup> Corte EDU, López Ribalda e altri v. Spagna, ricorsi nn. 1874/12 e 8567/13, 17 ottobre 2019 (Grande Camera), par.131; occorre ricordare che, nell'opinione della Corte, se il datore di lavoro avesse avvisato i dipendenti dell'installazione di telecamere nascoste, questi avrebbero smesso di compiere furti, “annullando”, in concreto, il senso della sorveglianza.

<sup>409</sup> Cfr. TUMMINELLO F., *Privacy sul posto di lavoro: la Corte EDU fa marcia indietro*, su <https://www.iusinitenere.it>; PISANU N., *Ok alle telecamere nascoste sul posto di lavoro in caso di furti: la sentenza della Corte UE*, su <https://www.cybersecurity360.it>; BREGIANNIS F., *López Ribalda and Others v. Spain – covert surveillance in the workplace: attenuating the protection of privacy for employees*, StrasbourgObserver, 6 dicembre 2019, su <https://strasbourgobservers.com/>.

di "gravi illeciti" e con modalità spaziotemporali tali da limitare al massimo l'incidenza del controllo sul lavoratore. Non può dunque diventare una prassi ordinaria. Il requisito essenziale perché i controlli sul lavoro, anche quelli difensivi, siano legittimi resta dunque, per la Corte, la loro rigorosa proporzionalità e non eccedenza: capisaldi della disciplina di protezione dati la cui "funzione sociale" si conferma, anche sotto questo profilo, sempre più centrale perché capace di coniugare dignità e iniziativa economica, libertà e tecnica, garanzie e doveri".

Nel suo conciso ma efficace comunicato stampa il Soro ha voluto fissare alcuni punti cardine della sentenza europea, per prevenire la sua possibile strumentalizzazione. Come riportato, ha in primo luogo aperto il comunicato affermando che la videosorveglianza occulta continua a essere una misura eccezionale da valutare caso per caso e applicare quale ultimo approdo. L'indagine sulla legittimità della misura di controllo, anche difensiva, non può che passare attraverso i principi di proporzionalità e non eccedenza. Quindi, non c'è alcuna liberalizzazione del controllo tecnologico occulto, ma un richiamo alla doverosità di applicare i già ricordati principi anche nel caso di controlli difensivi; controlli che per il loro grado d'invasività e di limitazione della sfera personale devono rimanere confinati nell'area della *extrema ratio*<sup>410</sup>.

Alla luce di queste considerazioni, in un quadro di costante progresso tecnologico e digitalizzazione, in cui i controlli effettuati, vuoi da autorità nazionali, vuoi da datori di lavoro, sono sempre più invasivi della riservatezza dei singoli, le pronunce della Corte EDU, qui analizzate, meritano attenzione e approfondimento, costituendo rilevanti spunti di riflessione per il legislatore e il giudice italiano<sup>411</sup>. In merito ai controlli del datore di lavoro, è da rilevare come in Italia, anche dopo la riforma dell'art. 4 dello Statuto dei lavoratori, il suo rapporto con il diritto alla riservatezza dei lavoratori e la tutela dei dati personali possa ancora presentare alcune zone d'ombra. In questo contesto, l'indirizzo della Corte EDU può certamente rivestire un ruolo importante per indirizzare i giudici nazionali verso un equo bilanciamento, nei casi più complessi.

---

<sup>410</sup> Cfr. BERTOCCO S., *La videosorveglianza occulta del lavoratore alla luce del 'nuovo' giudizio di bilanciamento della Corte Edu: la protezione di prevalenti interessi pubblici o privati*, su <https://www.massimariodellagiurisprudenzadellavoro.it>; MARINI P., *Controlli difensivi occulti: leciti se ragionevoli e proporzionati*, su <http://www.altalex.com>.

<sup>411</sup> Cfr. TURSI A.- VARESI P.A., *Istituzioni di Diritto del Lavoro*, Padova, 2016; PROIA G., *Trattamento dei dati personali, rapporto di lavoro e l'“impatto” della nuova disciplina dei controlli a distanza*, in *Rivista Italiana di Diritto del Lavoro*, 1/2016, pp. 547 ss.

## CONCLUSIONI

L'iniziale ricostruzione del concetto di controllo, impostata prendendo in prestito il modello di prigione teorizzato da Jeremy Bentham, piuttosto che l'espressione di Norberto Bobbio "*l'ideale di ogni potente è sempre stato quello di vedere ogni gesto e di ascoltare ogni parola dei suoi soggetti (possibilmente senza essere visto né ascoltato)*"<sup>412</sup> sono indici rivelatori della centralità che il controllo svolge da sempre nella società e permettono di osservare facilmente un fenomeno che, traslato nel diritto del lavoro al tempo dell'industria 4.0, consente di affermare che è, ed è sempre stata forte per i datori di lavoro la tentazione di un controllo senza freni sui propri dipendenti. D'altronde i datori di lavoro hanno sempre raccolto informazioni sui propri lavoratori subordinati, sia nella fase precontrattuale, di selezione dei contraenti, sia nella fase esecutiva dell'obbligazione, a tutela dei propri interessi più o meno legati all'organizzazione d'impresa come struttura di potere, struttura gerarchica; quello che è mutato rispetto al passato è l'incremento dei livelli di automazione nell'organizzazione del lavoro, che ha permesso di affinare le tecniche che consentono un controllo dei dipendenti. Oggi è tutt'altro che arduo per il datore di lavoro sorvegliare il proprio dipendente attraverso l'impiego delle nuove tecnologie, diventando sempre più stretta la relazione tra l'uomo e la macchina, tra svolgimento della prestazione lavorativa e apparecchiature tecnologiche utilizzate, in quanto nella maggior parte dei casi funzionali ai processi produttivi. È dunque essenziale verificare se il legislatore abbia introdotto efficaci regole e limiti a un controllo, potenzialmente smodato, sulla prestazione lavorativa.

Dal presente lavoro è emerso come oggi la digitalizzazione nei luoghi di lavoro abbia due sfaccettature: la tecnologia come strumento per i lavoratori, da un lato, e come *longa manus* del titolare del potere di controllo, dall'altro. In entrambi i casi, comunque, ciò che subisce, o rischia di subire, ingerenza e compressione è sempre la privacy del lavoratore.

In quest'ottica il presente elaborato ha analizzato l'art. 4 dello Statuto dei lavoratori, riformato dal d.lgs. n. 151/2015: è stata ricostruita l'evoluzione della complessa disciplina dei controlli a distanza dei lavoratori, nella sua intersezione con l'estensione del diritto alla privacy, senza tralasciare di tracciare il quadro normativo europeo e nazionale, alla luce del nuovo Regolamento europeo in materia di tutela delle persone fisiche n. 679 del 2016 (GDPR) e del d.lgs. n. 101/2018 contenente le disposizioni per l'armonizzazione delle norme enunciate dal nostro legislatore nel Codice in materia di protezione dei dati personali (d.lgs. n. 196/2003) con quelle introdotte dal Regolamento Europeo n. 679/2016.

---

<sup>412</sup> BOBBIO N., *Il futuro della democrazia*, Torino, 1984.

A distanza di cinquant'anni da quando per la prima volta nel nostro ordinamento l'art. 4 dello Statuto dei lavoratori ha disciplinato la materia dei controlli a distanza, questa norma fa ancora discutere; dall'enorme forza innovativa nel contesto in cui è nata, portatrice all'interno del nostro sistema di una certa tutela della privacy, di cui fino a quel momento non era stata riscontrata alcuna traccia, la disposizione è stata etichettata, ben prima di quello che il legislatore si potesse aspettare, come destinata all'obsolescenza, poiché scritta pensando a un certo tipo di lavoro e di strumentazione tecnologica, entrati in crisi già pochi anni dopo l'entrata in vigore dello Statuto.

Lo sviluppo tecnologico ha cambiato sia il modo in cui si era soliti guardare alla privacy, sia il modo in cui potevano essere eseguiti i controlli a distanza e inevitabilmente l'articolo 4 ha cominciato a perdere terreno; d'altronde più la tecnologia procede celermente, e più sarà difficile ancorarla a una norma che, per sua stessa natura, è statica nel fotografare la realtà di cui è figlia.

Il confronto tra il passato e il presente e l'analisi degli indirizzi dottrinali e giurisprudenziali *ante* e *post* riforma hanno permesso di rilevare come nel bilanciamento tra potere di controllo del datore di lavoro e diritto del lavoratore alla tutela della propria privacy, nessun interesse viene totalmente sacrificato a favore dell'altro, essendo entrambi meritevoli di protezione.

Al nuovo art. 4 dello Statuto dei lavoratori innegabilmente è da riconoscere il merito di aver fatto un balzo in avanti rispetto alla precedente impostazione statutaria, e, riconoscendo espressamente la tutela della riservatezza dei dati personali, e, prendendo coscienza del progresso tecnologico. Tuttavia, pur essendo cristallino il pregnante valore dell'intervento legislativo, è altrettanto innegabile che, nonostante tali innovazioni, di straordinaria portata, rimangano delle perplessità. La nuova disciplina dei controlli a distanza, infatti, non sembra essere atta a tutelare in modo definitivo la norma, e quindi la materia del controllo a distanza, dal rischio dell'obsolescenza provocata dallo sviluppo tecnologico ancora, inevitabilmente, *in fieri*, risultando così stare sempre un passo indietro, come se ogni riforma, volta a tener testa, in un certo senso, al costante fenomeno della crescente digitalizzazione che investe il mondo del lavoro, nascesse già obsoleta. Prova di ciò sono il fenomeno dei microchip impiantati su pelle che, se fino a qualche anno fa sembrava essere fantascienza, oggi in alcune aziende è realtà, nonché i vari cambi di orientamento registrati in seno alla giurisprudenza europea sulle tecnologie, quali la videosorveglianza e ancora la recente vicenda del braccialetto elettronico, firmato Amazon, un "bracciale intelligente" legato al polso dei lavoratori e brevettato, a dire dell'azienda, sostanzialmente per ottenere un processo produttivo migliore. Dispositivo che però, nella realtà, per le sue caratteristiche, ha sollevato dubbi sulla sua legittimità.

Questi richiamati esempi rendono lampante l'impossibilità di scoraggiare o arginare l'evoluzione tecnologica: prima si prende consapevolezza di ciò e prima sarà possibile rispondere alla necessità di individuare i contrappesi idonei a evitare i rischi del controllo totale e tutelare i diritti fondamentali, quale la dignità del lavoratore. In questo quadro, l'interprete sarà tenuto a prendere atto della facilità con cui l'inarrestabile evoluzione tecnologica causerà un'intensificazione di modalità e strumenti di controllo attualmente neanche concepibili e, dunque, difficilmente disciplinabili, non potendosi regolare ciò che non si può neanche ipotizzare; e la sua sfida sarà quella di capire in che modo il lavoratore possa essere tutelato nella digitalizzata realtà produttiva di volta in volta attuale.

Le considerazioni fin qui svolte dunque consentono di sposare l'analogia della materia dei controlli a distanza con un "*cantiere aperto, alla costante ricerca di un punto di equilibrio tra le prerogative del datore di lavoro e la privacy (e dignità) del lavoratore*"<sup>413</sup>.

---

<sup>413</sup> FABOZZI R., *I controlli a distanza (di cinquanta anni)*, su <http://www.massimariogiurisprudenzadellavoro.it/>.

## BIBLIOGRAFIA E SITOGRAFIA

- AGOSTINI C., *Dati personali dei lavoratori: il WP29 aggiorna le regole del trattamento alla luce delle nuove tecnologie informatiche e del GDPR*, in *Privacy & Data Protection*, 2017.
- AIELLO C., *Wisconsin company known for microchipping employees plans GPS tracking chip for dementia patients*, su <https://www.cnbc.com/>.
- AIMO M., *La c.d. cybersurveillance sui luoghi di lavoro*, in TULLINI P. (cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, Padova, 2010.
- ALVINO I., *L'art. 4 dello Statuto dei lavoratori alla prova di Internet e della posta elettronica*, in *Dir. rel. ind.*, 2014, n. 4, p. 1015.
- ALVINO I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in "Labour & Law Issues", vol. 2, no. 1, 2016.
- AMBROSINO A. – CASTIGIONE F., *Nuove forme di controllo a distanza dell'attività lavorativa: aspetti sostanziali e processuale della disciplina statutaria*, in *Lavoro e Previdenza oggi*, 2011.
- AMOROSO G. – DI CERBO V. – MARESCA A., *Diritto del lavoro. Lo statuto dei lavoratori e la disciplina dei licenziamenti*, Milano, 2017.
- ARENDT H., *Le origini del totalitarismo*, Torino, 2004.
- ARNOLD D.G. – BEAUCHAMP T.L. – BOWIE N. E., *Ethical Theory and Business*, Cambridge, 2020.
- ASSANTI C. - PERA G., *Commento allo Statuto dei diritti dei lavoratori*, Padova, 1972, p.17.
- BALLESTRERO M.V., *Le "energie da lavoro" tra soggetto e oggetto*, in WP C.S.D.L.E. "Massimo D'Antona" .IT - 99/2010.
- BALLESTRERO M.V. – DE SIMONE G., *Diritto del lavoro*, Torino, 2017.
- BALLETTI E., *I controlli a distanza dei lavoratori dopo il jobs act*, in SANTONI F.- RICCI M.- SANTUCCI R. (a cura di), *Il diritto del lavoro all'epoca del jobs act*, Napoli, 2016.
- BARASSI L., *Contratto di lavoro nel diritto positivo italiano*, Roma - Milano – Napoli, 1915.
- BARBIERI M., *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in TULLINI P., (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017.
- BARRACO E., *Utilizzo delle e-mail ed Internet da parte del dipendente per uso privato*, su [www.csdn.it/](http://www.csdn.it/).
- BARRACO E. – STIZIA A., *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milanofiori Assago (MI), 2016.

BARRACO E. – SITZIA A., *Il problema dei “controlli difensivi” del datore di lavoro: estne saepe ius summus malitia?*, in *Lav. giur.*, 2010, p. 993.

BELLAVISTA A., *Il controllo sui lavoratori*, Torino, 1995.

BELLAVISTA A., *I poteri dell’imprenditore e la privacy del lavoratore*, in *Dir. lav.*, 2002, I.

BELLAVISTA A., *Gli accordi sindacali in materia di controlli a distanza sui lavoratori*, in *Lav. giur.*, 2014, pp. 737 ss.

BELLAVISTA A., *Il nuovo art. 4 dello Statuto dei lavoratori*, in ZILIO GRANDI G.- BIASI M., *Commentario breve alla riforma del “Jobs Act”*, Padova, 2016.

BENTHAM J., *Panopticon, ovvero la casa d’ispezione*, FOUCAULT M.- PERROT M. (a cura di), Venezia, 1983.

BERNARDO P., *Vigilanza e controllo sull’attività lavorativa*, in CARINCI F., *Diritto del lavoro, Commentario*, Torino, 2007.

BERTOCCO S., *La videosorveglianza occulta del lavoratore alla luce del 'nuovo' giudizio di bilanciamento della Corte Edu: la protezione di prevalenti interessi pubblici o privati*, su <https://www.massimariodellagiurisprudenzadellavoro.it>.

BIESUZ E., *Lavoro autonomo e subordinato: le posizioni in dottrina e giurisprudenza*, su [www.lavoroprevidenza.com](http://www.lavoroprevidenza.com) – Osservatorio di Diritto del Lavoro e di Previdenza Sociale.

BOBBIO N., *Il futuro della democrazia*, Torino, 1984.

BOLOGNINI L., *Utilizzo di strumenti e di tecnologie con finalità di controllo dei lavoratori*, in convegno organizzato da Alta Formazione Giuridico-Economia (AGFE), *Privacy e controllo sui lavoratori alla luce dei decreti attuativi dei Jobs Act*, 22 marzo 2016, Roma.

BONACOSA P., *Datori di lavoro, nuove regole per effettuare i controlli in linea con la privacy*, in *Privacy – La Nuova disciplina europea, Guida normativa*, Il Sole 24 Ore, Febbraio 2018, pp. 114 ss.

BORGHI P. – MIELI G., *La tutela della privacy nel rapporto di lavoro: le interpretazioni del Garante, gli orientamenti della dottrina e della giurisprudenza, le indicazioni operative per le aziende*, Roma, 2000.

BORTONE R., *Sub art. 2*, in GIUGNI G. (diretto da), *Lo Statuto dei lavoratori. Commentario*, Milano, 1979.

BREGIANNIS F. – LÒPEZ RIBALDA AND OTHERS V. SPAIN – *covert surveillance in the workplace: attenuating the protection of privacy for employees*, *StrasbourgObserver*, 6 dicembre 2019, su <https://strasbourgobservers.com/>.

BRESCIANI I., *Le forme di controllo nello Statuto dei lavoratori: orientamenti giurisprudenziali e questioni di attualità*, su <https://www.dirittolavorovariazioni.com/>.

BRESCIANI I., Il potere di controllo del datore di lavoro sulla posta elettronica aziendale del lavoro (nota di commento a CEDU, sez. IV, 12 gennaio 2016, C-61496/08), su <https://www.dirittolavorovariazioni.com/>.

BUFFA F., *Il controllo datoriale delle comunicazioni elettroniche del lavoratore dopo la sentenza Barbulescu 2 della Cedu*, in *Questione giustizia - Osservatorio internazionale*, su <https://questionegiustizia.it/>.

BUFFA F. – DE GIORGI C., *Il potere disciplinare. Nel lavoro privato, nel lavoro pubblico contrattualizzato, nel pubblico impiego e nel settore militare*, Matelica (MC), 2007.

BUFFA F. - PERRONE F., *La rilevanza dell'informazione preventiva nei controlli a distanza sul luogo di lavoro*, su <https://www.questionegiustizia.it>.

BUSIA G., *Codici di deontologia e buona condotta, Commento all'art. 12, in Codice della privacy*, Commentario coordinato da ITALIA V., *Le nuove leggi amministrative*, 2004, p. 166.

CAIRO L., *Semplificazione delle procedure e controlli a distanza*, Milanofiori Assago (MI), 2016.

CALIFANO L. – FIORILLO V., *Videosorveglianza*, in BIFULCO R. – CELOTTO A. – OLIVETTI M.(a cura di), *Digesto delle discipline pubblicistiche*, Torino, 2015.

CAMPINI N., *“No al microchip nello scarpone”, operai in sciopero alla Fincantieri*, su <https://genova.repubblica.it/>.

CANESTRARI S. – FERRANDO G. - MAZZONI C.M. – RODOTÀ S. – ZATTI P. (a cura di), *Trattato di biodiritto. Il governo del corpo*, Milano, 2011.

CAPOBIANCO M., *Privacy e controlli a distanza: ultimi approdi normativi e giurisprudenziali*, su [www.salvisjuribus.it](http://www.salvisjuribus.it).

CARDACI F. – OLIVETTI S., *Il diritto alla riservatezza in Italia*, in <http://www.jus.unitn.it/>.

CARIGLINO F. – BENVENGNÙ A. – PARUZZO F., *Diritto dell'Internet*, Padova, 2016.

CARINCI M. T., *Il controllo a distanza dell'attività dei lavoratori dopo il “Jobs Act” (art. 23 D.Lgs. 151/2015): spunti per un dibattito*, in *Labour & Law Issues*, vol. 2, no. 1, 2016.

CARINCI MT., *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017.

CARTA C., *Corte europea dei diritti dell'uomo: la Grande Camera torna sul (e difende il) diritto alla privacy del lavoratore*, su <https://www.rivistalabor.it>.

CARNABUCI A. – CECCOLI P. – DE ROSA B. – MARIANI I. – MINIERI C. – RADAELLI P. – ZAPPÀ A. – ZUCCHETTI A., *Privacy e dati personali: problemi e casi pratici*, Milano, 2018.

CATAUDELLA A., *Commento all'art. 4*, in PROSPERETTI U. (diretto da), *Commentario allo Statuto dei lavoratori*, 1975, Milano, p. 89.

CATAUDELLA A., *Dignità e riservatezza del lavoratore (tutela della)*, in Enciclopedia giuridica Treccani, XI, 1989, p. 4.

CALZOLAIO S., *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, su <http://www.federalismi.it/>, 2017.

CAVOUKIAN A., *Privacy by Design*, Ottawa, 2009.

CAVOUKIAN A., *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D*, in Identity in the Information Society, vol. 3, 2010, pp. 247-251.

CAZZELLA A., *La definizione di "strumento di lavoro" ex art. 4 Stat. Lav. secondo il Garante della privacy*, su <http://www.diritto24.ilsole24ore.com/>.

CHIECO P., *Telelavoro e statuto dei lavoratori*, in Lav. inf., 1999, n. 12.

CIARAFONI A., *I controlli dei lavoratori nel contesto tecnologico: un difficile tentativo di bilanciamento d'interessi contrastanti*, su <https://www.iusinitinere.it/>.

CICCOTTI F., *Diritto di accesso del datore di lavoro e diritto alla riservatezza del lavoratore*, in Il Diritto del lavoro, Vol. 69, Fasc. 2, 1995.

CINQUE G., *Sull'ammissibilità e i limiti dei cd. controlli difensivi del patrimonio aziendale*, in Orient. Giur. lav., 2010, 616.

CIRIELLO A., *Videosorveglianza "occulta" sul luogo di lavoro: il caso López Ribalda e altri c. Spagna e la giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in Lavoro Diritti Europa, no. 3/2019, pp. 2 ss.

COMOGLIO P., *Le prove*, Torino, 2010, pp. 51 ss.

CONTE D., *Riflessioni sull'articolo 4 dello statuto dei lavoratori alla luce della consistenza trifasica del controllo*, in Lavoro e previdenza oggi, 1-2, 2017, p. 2

CORDEDDA G., *Controlli a distanza sull'attività dei lavoratori: l'interpretazione dell'art. 4 SL secondo la giurisprudenza recente*, in D&L-Riv. crit. dir. lav., 2007, p.1058.

COSATTINI L.A., *Le modifiche all'art. 4 Stat. Lav. sui controlli a distanza, tanto rumore; per nulla?*, in Lav. giur., n. 11/2015, 985.

COSTANTINI S., *Limiti all'iniziativa economica privata e tutela del lavoratore subordinato: il ruolo delle cd. "clausole sociali"*, in Ianus - Diritto e Finanza n. 5/2011, pp. 203-204.

CROTONDI F. (a cura di), *Diritto del lavoro e delle relazioni industriali*, Milanofiori Assago (MI), 2017.

D'ACQUISTO G. – NALDI M., *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017.

D'ANGELO G., *Carl Sanders: il creatore del microchip sottocutaneo che si pentì della sua invenzione*, su <https://www.sapereundovere.com/>.

DAGNINO E., *Tecnologie e controlli a distanza*, in *Diritto delle Relazioni Industriali*, 2015, n. 4, pp. 1004 – 1005.

DAGNINO E., *Il braccialetto di Amazon, facciamo chiarezza*, su <http://www.bollettinoadapt.it/>.

DAGNINO E., *La Cassazione penale sui controlli a distanza post Jobs Act: continuità del tipo di illecito*, in *Diritto delle Relazioni Industriali*, 2017, n. 1, pp. 181 – 187.

DE CAROLIS D. – LEONETTI P., *Dalla norma al caso concreto: come la Privacy by Design influenza le dinamiche del rapporto lavorativo*, su <https://www.altalex.com/>.

DELL'ERARIO A. – LOSITO A. – CELIBERTI M., *Controllo a distanza dipendenti: cellulare, tablet, computer aziendali*, su <https://www.theitaliantimes.it/>.

DELL'OLIO M., *Art. 4 St. Lav. ed elaboratori elettronici*, in *Dir. Lav.*, 1986, I.

DELPANO C., *Controlli difensivi: l'art. 4 Stat. lav. tra vecchio e nuovo testo*, su <http://www.bollettinoadapt.it>.

DEL PUNTA R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23 d.lgs. n. 151/2015)*, in *Riv. It. Dir. Lav.*, 2016, 1, I, pp. 77 ss.

DE LUCA TAMAJO R., *Presentazione della ricerca*, in DE LUCA TAMAJO R. – IMPERIALI R. – D'AFFLITTO R. – PISANI C. – ROMEI R. (a cura di), *Nuove tecnologie e tutela della riservatezza del lavoratore*, Milano, 1988.

DE LUCA TAMAJO R., *I Controlli sui lavoratori*, in ZILIO GRANDI G. (a cura di), *I poteri del datore di lavoro nell'impresa, Atti del Convegno di studi*, Venezia, 2003.

DE LUCA TAMAJO R. – MAZZOTTA O., *Commentario breve alle leggi sul lavoro*, Milanofiori Assago (MI), 2018.

DE MICCO L., *Schiavitù 2.0: nei magazzini di Amazon mancano solo le frustate*, su <https://www.dagospia.com>.

DEMICHELIS L., *Sorvegliati e contenti: così i social hanno realizzato la forma di controllo perfetta*, su [www.agendadigitale.eu/cultura-digitale/](http://www.agendadigitale.eu/cultura-digitale/).

DEMICHELIS L., *Bio-Tecnica. La società nella sua forma tecnica*, Napoli, 2008.

DEMICHELIS L., *Il modello-panopticon. Dalla Nsa al Jobs Act*, su [www.temi.repubblica.it](http://www.temi.repubblica.it).

DE MINICO G., *Codici di deontologia e buona condotta, Commento all'art. 12*, in *La protezione dei dati personali, Commentario al D. lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*, BAINCA M. – BUSNELLI F.D. (a cura di), *Le nuove Leggi Civili Commentate*, tomo I, Padova, 2007, pp. 271 ss.

DI FRANCESCO M., *Controllo a distanza e utilizzazione di impianti Gps*, in *Diritto & Pratica del Lavoro*, n. 10/2017.

DI MEO R., *Tecnologie e poteri datoriali: commento a margine del cd. braccialetto Amazon*, in *Labour & Law Issues*, vol. 4, no. 1, 2018, pp. 11-13.

EVANGELISTI D., *Jobs Act, l'occhio della Ue su microchip e braccialetti per controllare i lavoratori*, su <https://www.ilfattoquotidiano.it/>.

FABOZZI R., *I controlli a distanza (di cinquanta anni)*, su <http://www.massimariogiurisprudenzadellavoro.it/>.

FALCO W., *Legittimo il controllo sull'uso del pc aziendale e sugli accessi ad internet da parte dei dipendenti*, su <https://www.toffolettodeluca.it/>.

FAMELI E., *La rilevanza giuslavoristica dei social network, tra diritti dei lavoratori e prerogative datoriali di controllo*, su [www.rivistaitalianadiinformaticaediritto.it](http://www.rivistaitalianadiinformaticaediritto.it).

FAVA G., *I braccialetti di Amazon: una possibile nuova forma di controllo dei lavoratori?*, su <https://www.4clegal.com>.

FERRANTE V., *Controllo sui lavoratori, difesa della loro dignità e potere disciplinare*, in *RIDL*, 1/2011, pp. 73 ss.

FERRARA F. – PAGLIARI F., *Limiti dei controlli difensivi sul lavoratore alla luce delle ultime pronunce della Corte di Cassazione*, su [www.filodiritto.com](http://www.filodiritto.com).

FLOR R., *Diritto penale e controlli a distanza dei lavoratori dopo il Jobs Act*, in LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza*, Milano, 2016.

FONTANA A., *In tema di "controlli a distanza"*, in *Dir. lav.*, 1985, II, p.202.

FORMICI G., *Lavoratori e tutela della privacy: l'evoluzione della giurisprudenza della Corte europea dei diritti dell'uomo, tra controllo della corrispondenza elettronica e videosorveglianza*, in *Osservatorio Costituzionale*, Fasc. 1/2018.

FOSSATI C. - MORPURGO C., *Internet e azienda*, in *Dir. prat. lav.*, 2001, n. 1, Inserto, III.

FOUCAULT M., *Sorvegliare e punire. Nascita della prigione*, Torino, 1975.

FOUCAULT M., *Sorvegliare e punire*, Torino, 2008.

FREDIANI M., *Abuso di accesso ad internet e potere di controllo datoriale*, in *Lav. giur.*, 2002, 947.

FRENI A. – GIUGNI G., *Lo Statuto dei lavoratori*, Milano, 1971.

GAMBA C., *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove*, in *Labour&Law Issues*, Vol. 2, n. 1, 2016.

GHEZZI G., *Computer e controllo dei lavoratori*, in *Giorn. Dir. lav. rel. ind.*, 1986, pp. 358 ss.

GHEZZI G. – ROMAGNOLI U., *Il rapporto di lavoro*, Bologna, 1987.

GIANNETTI L., *Una prigione di telecamere, un Panopticon moderno?*, su [www.ilsuperuovo.it](http://www.ilsuperuovo.it).

GILLIES T., *Why most of Three Square Market's employees jumped at the chance to wear a microchip*, su <https://www.cnbc.com/>.

GIUSTI F., *Videosorveglianza: il Panopticon del XXI secolo*, su [www.cittafutura.it/economia e lavoro/](http://www.cittafutura.it/economia-e-lavoro/).

GIUSTO N., *Foucault, Panopticon e ordine disciplinare*, su [www.culturedigitali.org](http://www.culturedigitali.org).

GOFFREDO M. T. – MELECA V., *Jobs Act e nuovi controlli a distanza*, in *Diritto & Pratica del Lavoro* n. 31/2016 p.1894 ss.

GRAGNOLI E., *L'uso della posta elettronica sui luoghi di lavoro e la strategia di protezione elaborata dall'autorità garante*, in Tullini P. (a cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali*, in *Trattato di diritto commerciale e diritto pubblico dell'economia*, diretto da GALGANO F., Padova, 2010.

GRANDI M., *"Il lavoro non è una merce": una formula da rimeditare*, in *Lavoro e diritto*, 1997.

GRANDI M., *Impianti di videosorveglianza in ambienti di lavoro. Autorizzazione ad installazione ed uso*, Milanofiori Assago (MI), 2017.

GROTTO M., *La rilevanza penale del controllo datoriale attraverso gli strumenti informatici*, in *Dir. inf.*, 2014, p. 57.

IASELLI M. – GORLA S., *"Storia della Privacy"*, Roma, 2015.

IBBA F. G., *GDPR, Il rapporto tra privacy, trasparenza amministrativa e accountability*, in *Agenda Digitale*, 2018.

ICHINO P., *Il contratto di lavoro*, Milano, 2003.

ICHINO P., *Il contratto di lavoro*, in CICU A. – MESSINEO F., *Trattato di diritto civile e commerciale*, III, Milano, 2003.

ICHINO P., *Lezioni di Diritto del lavoro*, Milano, 2004.

ILIAS VIGLIOTTI G., *Controlli a distanza e tutela della privacy del lavoratore: la CEDU conferma le scelte del legislatore interno. Nota a sentenza CEDU, sez. IV, 12 gennaio 2016, n. 61496/08*, in *Massimario di giurisprudenza del lavoro*, 4/2016, pp.211 ss.

IMPERIALI R. – IMPERIALI R., *Controlli sul lavoratore e tecnologie*, Milano, 2012.

INGRAO A., *Il controllo a distanza realizzato mediante Social network*, in *Labour & Law Issues*, 2016, vol.2, no. 1, p.110.

- INGRAO A., *Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy*, in *Labour & Law Issues*, vol. 5, n. 2, 2019, p. 138.
- INGRAO A., *Il “cyberslacking” e i diritti del lavoratore “catturato nella rete informatica”. Note critiche a margine della sentenza della Corte Europea dei diritti dell’Uomo, sez. IV, 12 gennaio 2016, n. 61496, Bărbulescu vs. Romania, in attesa della pronuncia della Grande Camera*, su <https://www.osservatorioaic.it/>.
- IAQUINTA F. – INGRAO A., *La privacy e i dati sensibili del lavoratore legati all’utilizzo di social networks. Quando prevenire è meglio che curare*, *DRI*, 2014, p.1027.
- JAMES D., *“Salt, Sir Titus, first baronet (1803–1876)”*, *Oxford Dictionary of National Biography*, Oxford University Press, 2004.
- KIRSCHEN S., *Il codice della privacy, fra tradizione ed innovazione*, in PANETTA R. (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006.
- LAI M., *Utilizzo dei social in ambito di lavoro*, in *Diritto e pratica del lavoro* 5/2020 pp. 290 – 291.
- LAMBERTUCCI P., *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli “a distanza” tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs Act)*, in WP CSDLE “Massimo D’Antona” IT, 255/2015.
- LAMBROU M., *Geolocalizzazione dei veicoli aziendali*, in *Diritto e pratica del lavoro*, 5/2018, pp. 297 ss.
- LEVI A., *Il controllo informatico sull’attività del lavoratore*, Torino, 2013.
- LEVI A., (a cura di) *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei lavoratori dopo il Jobs Act*, Milano, 2016.
- LISO F., *Computer e controllo dei lavoratori*, *Giorn. dir. lav. e rel. ind.*, 1986, pp. 366 ss.
- LISO F., *Brevi osservazioni sulla revisione della disciplina delle mansioni contenuta nel decreto legislativo n° 81/2015 e su alcune recenti tendenze di politica legislativa in materia di rapporto di lavoro*, in Working Papers “Massimo D’Antona” n. 257/2015 in <http://csdle.lex.unict.it>.
- LOMARDI A., *Il potere di controllo del datore di lavoro alla luce della giurisprudenza CEDU*, Ricerca del Dipartimento di Diritto Pubblico dell’Università di Perugia, 18 novembre 2017.
- LONGO A., *GDPR – Tutto ciò che c’è da sapere per essere in regola*, su <https://www.agendadigitale.eu/>.
- LORÈ F., *La tutela della privacy nell’esercizio del potere datoriale*, fascicolo n. 1/2020, su [www.amministrativamente.com](http://www.amministrativamente.com).
- LYON D., *L’occhio elettronico. Privacy e filosofia della sorveglianza*, Milano, 1997.

MAINARDI S., *Le relazioni collettive nel “nuovo” diritto del lavoro*, relazione nell’ambito delle giornate di studio AIDLASS, Napoli, 16-17 giugno 2016, dattiloscritto, p. 43.

MAIO V., *La nuova disciplina dei controlli a distanza sull’attività dei lavoratori e la modernità post panottica*, in Arg. Dir. Lav., 2015, 6, pp. 1186 ss.

MAIO V., *Il regime delle autorizzazioni del potere di controllo del datore di lavoro ed i rapporti con l’art. 8 della legge n. 148/2011*, in TULLINI P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino 2017.

MALET J.B., *En Amazonie. Un infiltrato nel “migliore dei mondi”*, Roma, 2013.

MANNINO V., *Introduzione alla storia del diritto privato dei Romani*, Torino, 2011.

MANTOVANI R., *Impiegati col chip sottopelle*, su <https://www.focus.it/>.

MARAZZA M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in Working papers CSDLE “Massimo D’Antona”.IT - 300/2016.

MARAZZA M., *Comportamenti illeciti del lavoratore e poteri sanzionatori del datore di lavoro*, in convegno organizzato da Alta Formazione Giuridico-Economia (AGFE), *Privacy e controllo sui lavoratori alla luce dei decreti attuativi dei Jobs Act*, 22 marzo 2016, Roma.

MARAZZA M., *I controlli a distanza del lavoratore di natura “difensiva”*, in TULLINI P.(a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino 2017.

MARESCA A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in TULLINI P., (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017.

MARESCA A., *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore*, in Forum Tuttolavoro (web), 2016.

MARINI P., *Controlli difensivi occulti: leciti se ragionevoli e proporzionati*, su <http://www.altalex.com>.

MARX K., *Il Capitale*, Libro I, Torino, 2011.

DE BONI C. (a cura di), *Lo stato sociale nel pensiero politico contemporaneo: L'Ottocento*, Firenze, 2007.

MAZZOTTA O., *Diritto del lavoro*, Milano, 2013.

MENGONI L., *L’evoluzione del pensiero di L. Barassi dalla prima alla seconda edizione del “contratto di lavoro”*, in Id. *Il contratto di lavoro* di NAPOLI M., Milano, 2004.

MISCHITELLI L., *Videosorveglianza e GDPR, i consigli e gli esempi nelle linee guida EDPB*, su <https://www.cybersecurity360.it/>.

MISCIONE M. – RAUSEI P., *Interpelli lavoro. Rassegna commentata degli anni 2005 e 2006*, Milanofiori Assago (MI), 2007.

MISCIONE M., *Dialoghi di diritto del lavoro*, Milano, 2011.

MONTEMANARO A., *Il codice di comportamento dei dipendenti pubblici*, in Guida lav., 2013, n. 27.

MORTATI C., *Commento all'art. 1 della Costituzione*, in *Commentario della Costituzione*, BRANCA C. (a cura di), 1° Vol., Artt. 1-12: principi fondamentali, Bologna, 1975.

NAPOLI M., *La stabilità reale del rapporto di lavoro*, Milano, 1982.

NAPOLI M., *Le norme costituzionali sul diritto del lavoro alla luce dell'evoluzione del diritto del lavoro*, in Scritti in onore di Edoardo Ghera, Bari, 2008.

NOGLER L., *Sulle contraddizioni logiche della cassazione in tema di diritto alla riservatezza del lavoratore subordinato*, in Resp. civ. prev., 1998, 111.

PADOVANI T., *Il controllo a distanza dell'attività lavorativa svolta mediante elaboratori elettronici*, in Riv. It. Dir. Lav., 1985, II, p.252.

PAGALLO U., *La tutela della privacy negli Stati Uniti d'America ed in Europa*, Milano, 2008.

PAGALLO U., *Privacy e design*, in *Informatica e diritto*, vol. XVIII, no. 1, 2009.

PAISSAN M., *Email e navigazione in internet: le linee guida del Garante*, in TULLINI P., *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, Padova, 2010.

PALOMEQUE LÓPEZ M. – ÁLVAREZ DE LA ROSA M., *Derecho del Trabajo*, Madrid, 2019.

PAMPALONE E., *La videosorveglianza in Europa: un fragile equilibrio tra "controllo" e "libertà"*, in TORRE A. (a cura di), *Costituzioni e sicurezza dello Stato*, Santarcangelo di Romagna, 2013.

PARKER C. – VONOWSU B., *AMAZON employees are exposed to such gruelling working conditions, they fall asleep on their feet, it has been claimed*, su <https://www.thesun.co.uk/>.

PASSALACQUA P., *Il modello del sindacato comparativamente più rappresentativo nell'evoluzione delle relazioni sindacali*, in Dir. rel. ind., 2014, pp. 375 ss.

PECCHIOLI R., *La società della sorveglianza. Totalitarismo del terzo millennio*, su [www.ariannaeditrice.it](http://www.ariannaeditrice.it).

PERA G. (ASSANTI C.) *Commento allo Statuto dei diritti dei lavoratori*, Padova, 1972.

PERONE G.C., *Lo Statuto dei Lavoratori*, su [www.shop.wki.it/editore/utet\\_giuridica](http://www.shop.wki.it/editore/utet_giuridica).

PERRONE F., *Corte Europea dei Diritti dell'Uomo, sentenza López Ribalda c. Spagna: la tutela della privacy sul luogo di lavoro dopo Bărbulescu 2*, su <https://www.rivistalabor.it>.

PERRUCCHIETTI E., *Braccialetti elettronici e microchip. Storie di schiavi e di infiltrati in Amazon*, su <https://rivoluzione.unoeditori.com/>.

PERRUCCHIETTI E., *Tutti controllati col chip sottopelle*, su <https://www.ariannaeditrice.it/>.

PERULLI A., *Il controllo giudiziale dei poteri dell'imprenditore tra evoluzione legislativa e diritto vivente*, in Riv. it. dir. lav., 2015, n.1, I, pp. 83 ss.

PESSI R., *Impresa e diritto del lavoro*, in Gnosis – Rivista italiana di intelligence n.4/2008.

PESSI R., *Lezioni di diritto del lavoro*, Torino, 2016.

PICA T., *DPIA, quando è obbligatoria e chi sono i soggetti coinvolti*, su <https://www.cybersecurity360.it/>.

PISANI C., *I controlli a distanza sui lavoratori*, in DLRI, 1987, pp. 121 ss.

PISANI C., *La nuova disciplina del mutamento delle mansioni*, Torino, 2015.

PISANI C., *Il computer e l'art. 4 dello Statuto dei lavoratori*, in FRANCO ANGELI, *Nuove tecnologie e tutela della riservatezza dei lavoratori*, 1998, p. 43.

PISANU N., *Ok alle telecamere nascoste sul posto di lavoro in caso di furti: la sentenza della Corte UE*, su [https://www.cybersecurity360.it](https://www.cybersecurity360.it/).

PITITTO E. A., *Il "nuovo" art. 171 del Codice Privacy: oltre la razionalizzazione normativa?*, su <http://www.bollettinoadapt.it/>.

PONTI C., *Le fattispecie penali alla luce del novellato Codice Privacy: il quadro*, su <https://www.agendadigitale.eu/>.

PROIA G., *Trattamento dei dati personali, rapporto di lavoro e l'"impatto" della nuova disciplina dei controlli a distanza*, in Rivista Italiana di Diritto del Lavoro, 1/2016, pp. 547 ss.

PROSPERETTI G., *Dalla tutela del rapporto di lavoro*, in Riv. Infortuni, 1994 p. 4.

RESTA G., *Il diritto alla protezione dei dati personali*, in CARDARELLI F. – SICA S. – ZENOVICH V. (a cura di), *Il codice dei dati personali, temi e problemi*, Milano, 2004.

RICCIO R., *La problematica disciplina della geolocalizzazione dei dispositivi aziendali*, su <https://www.cyberlaws.it/>.

RICCIO G.M. – SCORZA G. – BELISARIO E. (a cura di), *GDPR e normativa privacy. Commentario*, Milanofiori Assago (MI), 2018.

RIZZI R. – VENTURA A., *La tutela della privacy del lavoratore controllato a distanza*, Consiglio e La Fondazione Nazionale dei Dottori Commercialisti.

ROCCHINI E., *Social network e controlli a distanza. Alla ricerca di un difficile equilibrio*, su <http://www.massimariogiurisprudenzadellavoro.it/>.

RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995.

ROMAGNOLI U., *Art. 4*, in SCIALOJA A., G. BRANCA G. (a cura di), *Statuto dei diritti dei Lavoratori*, Roma – Bologna, 1979.

ROMAGNOLI U., *Il lavoro in Italia*, Bologna, 1995.

ROMAGNOLI U., *Sub art. 4*, in GHEZZI G. – MANCINI G.F. – MONTUSCHI L. – ROMAGNOLI U., *Statuto dei diritti dei lavoratori*, Bologna, 1972.

ROMANI R., *Braccialetto elettronico e controllo a distanza del lavoratore. Il caso Amazon*, su <https://www.altalex.com>.

ROTA A., *Rapporto di lavoro e big data analytics: profili critici e risposte possibili*, in LLI, 2017, 3, n. 1, 34 ss.

RUSSO E., *Statuto dei lavoratori: nozioni, limiti e possibilità di deroghe*, in QFMB Saggi, 2013 n° 2.

SALIMBENI M.T., *Sub art. 4*, in DE TAMAJO – MAZZOTTA O., *Commentario breve alle leggi sul lavoro*, Padova, 2013.

SALIMBENI M.T., *La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in Riv. It. Dir. Lav., 2015, 4, I, pp. 589 ss.

SALIOLA S., *Il caso Soraya e l'applicazione diretta della CEDU*, su <http://www.iurisprudentes.it/>.

SALVI N.M., *Controlli a distanza e consenso dei lavoratori: la Cassazione fa dietrofront*, su <https://www.altalex.com/>.

SANTONI F., *La revisione della disciplina dei rapporti di lavoro*, in F. CARINCI (a cura di), *La politica del lavoro del Governo Renzi. Atto II*, Adapt Labour Studies, n. 32, 2014, pp.116 ss.

SANTORO PASSARELLI F., *Spirito del diritto del lavoro*, in *Saggi di diritto civile*, Napoli, 1959.

SANTORO PASSARELLI G., *Diritto dei lavori e dell'occupazione*, Torino, 2017.

SCOGNAMIGLIO R., *Contratto di lavoro e prestazione d'opere*, in NAPOLI M. (a cura di), *La nascita del diritto del lavoro, "Il contratto di lavoro" di Lodovico Barassi cent'anni dopo. Novità, influssi, distanze*, Milano, 2003.

SELBY A., *Timed toilet breaks, impossible targets and workers falling asleep on feet: Brutal life working in Amazon warehouse*, su <https://www.mirror.co.uk/>.

SITZIA A., *Il diritto alla privacy nel rapporto di lavoro tra fonti comunitarie e nazionali*, Padova, 2013.

SITZIA A., *I controlli a distanza dopo il "Jobs Act" e la Raccomandazione R(2015)5 del Consiglio d'Europa*, in LG, 2015, pp. 671 ss.

SITZIA A., *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore)*, vol. 2, no. 1, 2016.

SITZIA A. - PIZZONIA D., *Il controllo del datore di lavoro su internet e posta elettronica: quale riservatezza sul luogo di lavoro?*, in Nuova Giur. Civ., 6/2016, 899.

SMITH M. – COATES C., *Salts Mill: The Owners and Managers 1853 to 1986*, Gloucestershire, 2016.

SOFFIENTINI M., *Privacy, protezione e trattamenti dei dati*, Milanofiori Assago (MI), 2016.

SOFFIENTINI M., *Geolocalizzazione e impatto privacy*, in *Diritto e pratica del lavoro*, 17/2017 p.889 ss.

SOFFIENTINI M., *Videosorveglianza sul lavoro e privacy*, Milanofiori Assago (MI), 2018.

SORO A., *I lavoratori devono essere informati. Il datore di lavoro non può spiare le mail*, in *L'Huffington post*, 13 gennaio 2016.

SPEZIALE V., *Le politiche del lavoro del governo Renzi: il Jobs Act e la riforma dei contratti e di altre discipline del rapporto di lavoro*, in WP C.S.D.L.E. “Massimo D’Antona”. IT, n. 233/2014, pp. 37 ss.

SPINELLI G., *La legittimità dei controlli datoriali cd. “difensivi”: certezze apparenti in una categoria dubbia*, in *Riv. it. dir. lav.*, 2013, n.1, II, 2016.

STANCHI A., *Privacy, rapporto di lavoro, monitoraggio degli accessi a Internet, monitoraggio delle e mail, e normative di tutela contro il controllo a distanza. Alcuni spunti per una riflessione interpretativa*, in A.A.VV., *I poteri del datore di lavoro nell’impresa*, Padova, 2002.

STENICO E., *La tutela della riservatezza del lavoratore nell’esercizio della prestazione*, in *Quad. dir. lav. e rel. ind.*, 2000, n. 24, p.169.

STURMAN C., *Three Square Market hopes to use its microchipping technologies for vulnerable patients*, su <https://www.healthcareglobal.com/>.

TEBANO E., *Amazon brevetta un braccialetto elettronico che monitora i lavoratori*, su <https://www.corriere.it/>.

TEBANO L., *Tutela della privacy e potere di controllo del datore di lavoro tra l’ordinamento italiano e le fonti europee*, in *Labour&Law Issues*, 2/2017.

TESTA D.M. – PICCARI M. (con la collaborazione di), *“Grande fratello” in azienda con la legge 183/2014 (c.d. Jobs act) : profili di riflessione*, su [www.iurisprudentes.it](http://www.iurisprudentes.it).

TIRABOSCHI S., *Controllo a distanza e procedimento di autorizzazione amministrativa: i chiarimenti del Ministero del Lavoro in ordine al silenzio amministrativo*, su <http://www.bollettinoadapt.it/>.

TORRENTE A. – SCHLESINGER P., *Manuale di diritto privato*, Milano, 2015.

TOSSERI O., *Ca se passe en Europe : en Italie, levée de boucliers contre le bracelet d'Amazon*, su <https://www.lesechos.fr/monde/europe/>.

TRENTIN B., *La città del lavoro: sinistra e crisi del fordismo*, Milano, 1997.

TREU T., *Condotta antisindacale e atti discriminatori*, Milano, 1974.

TROJSI A., *Il diritto del lavoratore alla protezione dei dati personali*, Torino, 2013.

TROJSI A., *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, su <http://www.dirittolavorovariazioni.com/>.

TUFO M., *I nuovi controlli a distanza tra tecnologie informatiche e privacy del lavoratore* in BASENGHI F. – RUSSO A., *Flessibilità, sicurezza e occupazione alla prova del Jobs Act*, Torino, 2016.

TULLINI P., *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in *Dir. lav. rel. ind.*, 2009, n. 3, I, pp. 323 ss.

TULLINI P., *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. Uso di mezzi elettronici, potere di controllo e trattamento dei dati personali*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Padova, 2010.

TULLINI P. (a cura di), *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in *Web e lavoro, Profili evolutivi e di tutela*, Torino, 2017.

TUMMINELLO F., *Privacy sul posto di lavoro: la Corte EDU fa marcia indietro*, su <https://www.iusinitenere.it>.

TURSI A. – VARESI P.A., *Istituzioni di Diritto del Lavoro*, Padova, 2016.

VALLEBONA A., *Commento agli artt. 1, 2 e 8*, in GRANDI M. – PERA G., *Commentario breve allo Statuto dei lavoratori*, Padova, 1985.

VAN DEN HOVEN VAN GENDERN R., *Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics*, in *European Data Protection Law Review*, 2017, III, pp. 338 ss.

VARANI E., *Il "nuovo diritto" alla privacy. Dalla Carta di Nizza al "Codice in materia di protezione dei dati personali"*, su <https://www.filodiritto.com/>.

VENEZIANI B., *I controlli dell'imprenditore ed il contratto di lavoro*, Bari, 1975.

VENEZIANI B. *Commento agli artt. 4 e 6*, in GIUGNI G. (diretto da), *Lo Statuto dei Lavoratori, Commentario*, 1979, Milano.

VILLA E., *Accordo sindacale e procedura amministrativa nei controlli a distanza dei lavoratori*, su <http://www.dirittolavorovariazioni.com/>.

ZAMPONI F., *Videosorveglianza sui luoghi di lavoro tra riforme normative e evoluzioni interpretative*, su <https://www.diritto.it/>.

WEISHAUPT G., *Amazon will jeden Handgriff seiner Mitarbeiter überwachen*, su <http://www.handelsblatt.com/unternehmen/handelskonsumgueter/armbaender-fuer-angestellte-amazon-will-jeden-handgriff-seiner-mitarbeiterueberwachen/.html>.

YEGINSU C., *¿Una pulsera para controlar los movimientos de los trabajadores?*, su <https://www.lanacion.com.ar/una-pulsera-para-controlar-los-movimientos-de-lostrabajadores>.

ZOLI C., *I licenziamenti per ragioni organizzative: unicità della causale e sindacato giudiziale*, in Arg. dir. lav., n.1, I, 2008, pp.31 ss.

ZOLI C., *Il controllo a distanza del datore di lavoro: l'art. 4 l. n. 300/1970 tra attualità ed esigenze di riforma*, in Riv. dir. it. lav., 2009, I, pp. 485 ss.

Comunicato stampa del Ministero del lavoro del 18 giugno 2015, *“Controlli a distanza: Ministero del lavoro, nessuna liberalizzazione; norma in linea con le indicazioni del Garante della Privacy”*, su <https://www.lavoro.gov.it/>.

Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a. - 11 settembre 2014, in <https://www.garanteprivacy.it/>.

Trattamento di dati personali mediante un sistema di localizzazione geografica dei dispositivi aziendali - 18 aprile 2018, in <https://www.garanteprivacy.it/>

## GIURISPRUDENZA

Cass., 21 febbraio 2006, n.4171, su <http://www.dirittolavoro.org/>.

Cass., 2 maggio 2012, n. 6643, su <http://adapt.it/>.

Cass., 8 febbraio 2010, n. 2728, in Arg. Dir. Lav., 2010, p. 943.

Cass., 10 marzo 2011, n. 5712, su <http://www.gadit.it/>.

Cass., 19 aprile 2010, n.9215 su <https://www.diritto.it/> con nota di MARAGA R.

Cass. 17 giugno 2000 n. 8250, su <https://www.unioncamere.gov.it/>.

Cass., 17 luglio 2007, n. 15892, in Riv. It. Dir. Lav., 2008, n. 3, II, 714 ss., con nota di VALLAURI M.L.

Cass., 17 luglio 2007, n. 15892, in RGL, 2008, II, P.358, con nota di BELLAVISTA A.

Cass., 8 ottobre 1985, n.8687 (ud. 28 maggio 1985), in Mass. Giur. Lav., 1986, p.404, con nota di PAPALEONI M.

Cass., 27 novembre 1992, n. 12765, in Riv. Giur. lav., 1993, II, con nota di PETRACCI F.

Cass., 9 giugno 1990, n. 5599, in Dir. e Prat. Lav., 1990, 1946.

Cass., 9 luglio 2008, n.18821, in Mass. Giur. It., 2008.

Cass., 5 maggio 2000, n. 5629, su <https://www.unioncamere.gov.it/>.

Cass., 18 febbraio 1997, n. 1455, in Giust. civ., 1997, I, 1261.

Cass., 9 giugno 1989, n. 2813, in Notiz. Giur. Lav., 1989, 289.

Cass., 17 ottobre 1998, n. 10313, su <http://dirittolavoro.altervista.org/>.

Cass., 14 luglio 2001, n. 9576, in Lavoro giur. 2002, 237.

Cass., 3 luglio 2001, n. 8998, su <https://www.avvocato.it/>.

Cass., 12 agosto 1998, n. 7933, in Notiz. Giur. Lav., 1998, 697.

Cass., 28 gennaio 2011, n. 2117, su <http://www.studiocesarerosso.it/>.

Cass., 4 aprile 2012 n. 5371, su <http://www.avvocatomandico.it/>.

Cass., 3 aprile 2002, n. 4746, su <https://www.altalex.com/>.

Cass., 4 dicembre 2014, n. 25674, in Foro it., 2015, I, c. 1671

Cass., 1 ottobre 2012, n.16622, su <http://adapt.it/>.

Cass., 23 febbraio 2012, n. 2722, su <http://www.avvocatomandico.it/>.

Cass., 23 febbraio 2010, n. 4375, su <https://www.ricercagiuridica.com/>.

Cass., 27 maggio 1975, n. 2129, su <https://protezionedatipersonali.it/>.

Cass., 22 ottobre 2002, n. 42217, in Dir. prat. lav., 2002, 506.

Cass. 18 febbraio 1983, n. 1236, in Giust. civ., 1983, I, 1755.

Cass. 9 febbraio 2016, n.2531, su <https://www.studiocerbone.com/>.

Cass. 16 settembre 1997, n.9211, in MGL, 1997, 804.

Cass., 14 luglio 2017, n. 17531, su <https://www.studiocerbone.com/>.

Cass. 10 ottobre 2012, n. 16622, in Not. giur. lav., 2012, p. 462

Cass., 31 gennaio 2017, n.22148, in GiustiziaCivile.com, fasc. 7 febbraio 2018.

Cass., 8 settembre 2016, n. 51897, su <https://www.eius.it/>.

Cass., 8 maggio 2017, n. 22148, su <https://www.studiocerbone.com/>.

Cass., 5 luglio 2016, n. 13663, su <https://giuricivile.it/>.

Cass., 2 settembre 2015, n. 17440, su <https://www.altalex.com/>.

Cass., 24 agosto 2018, n. 38882, su <http://www.lavorosi.it/>.

Cass., 24 agosto 2018, n. 38884, su <https://olympus.uniurb.it/>.

Cass., 30 gennaio 2014, n. 4331, su <https://olympus.uniurb.it/>.

Cass., 27 maggio 2015, n. 10955, in [www.ilgiuslavorista.it](http://www.ilgiuslavorista.it).

Cass., 1° agosto 2013, n. 18443, su <https://www.miolegale.it/>.

Cass. 11 giugno 2012 n. 2261, su <https://www.altalex.com/>.

Corte EDU, Niemietz contro Germania, 16 dicembre 1992, Grande Camera, ricorso n. 13710/88, su <https://hudoc.echr.coe.int/>

Corte EDU, Bărbulescu v. Romania, 12 gennaio 2016, sez. IV, ricorso n. 61496/08, su <https://hudoc.echr.coe.int/>.

Corte EDU, Bărbulescu v. Romania, 5 settembre 2017, Grande Camera, ricorso n. 61496/08, su <https://hudoc.echr.coe.int/>.

Corte EDU, López Ribalda e altri v. Spagna, 9 gennaio 2018, sez. III, ricorsi nn. 1874/13 e 8567/13, su <https://hudoc.echr.coe.int/>.

Corte EDU, López Ribalda e altri v. Spagna, 17 ottobre 2019, sez. III, ricorsi nn. 1874/13 e 8567/13, su <https://hudoc.echr.coe.int/>.

Corte EDU, Antovič e Mirkovič v. Montenegro, 28 novembre 2017, sez. II, ricorso n. 70838/13, su <https://hudoc.echr.coe.int/>.

Corte EDU, Köpke v. Germania, 5 ottobre 2010, Grande Camera, ricorso n. 420/07, su <https://hudoc.echr.coe.int/>.

Pret. Milano, 4 ottobre 1988, in Not. giurisp. lav. 1989, p. 436.

Pret. Firenze, 20 marzo 1990, in Orient. giur. lav., 1993, p. 5.

Pret. Milano, 1 marzo 1993, in Orient. giur. lav., 1994.

Pret. Milano, 5 dicembre 1984, in Foro it., 1985, p. 285.

Pret. Monopoli, ordinanza 27 ottobre 1970, in Foro it., 1971, I, 1060.

Trib. Napoli, 29 settembre 2010, in Riv. it. dir. lav., 2011, II, 31, con nota di FUSCO F.

Trib. Pordenone, 27 giugno 2014, in BARRACO E. – STIZIA A., *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milanofiori Assago (MI), 2016.

Trib. Roma, 24 marzo 2017, su <https://www.defensis.it/>.

App. Milano, 30 settembre 2005, in D&L, 2006, p. 899.